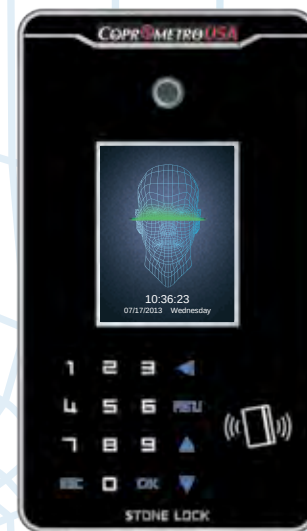


COPROMETROUSA®



Patent Pending

Stone Lock® Pro User Manual
v. 1.3



Preface

Thanks for choosing Stone Lock® Pro for your access control solution!

This User Manual had been developed as a reference to help the user enjoy
the ultimate in security + convenience with Stone Lock® Pro.

Modifications to the information in this Manual may occur without notification. For the latest
information about Stone Lock® Pro please visit our website at www.stonelockpro.com.

Stone Lock® Pro User Manual v1.3

Copyright © 2015 CoprometroUSA®

All Rights Reserved. This book or any portion thereof may not be reproduced or used in any manner whatsoever without the express written permission of CoprometroUSA® except for excerpts referred to or otherwise called out in the normal course of business operations.

© 2015 HID Global Corporation/ASSA ABLOY AB. All Rights Reserved.

HID, HID Global, the HID Blue Brick logo, the Chain Design and HID Connect iCLASS, iCLASS SE, are trademarks or registered trademarks of HID Global.

Designed in Leawood ∞ Printed in the USA

First Printing 2015

www.coprometrousa.com

Table of Contents

1.0 Introduction

Pg.

1.01.... Welcome to Stone Lock® Pro / Features.....	2
1.02.... Passive Interface.....	3
1.03.... What's in the Box?.....	4
1.04.... Preparation for Installation.....	5
1.05.... Locks	5
1.06.... Stone Lock® Network Platform.....	5
1.07.... Installation Checklist	6
1.08.... Installation	8
1.09.... Connecting Stone Lock® Pro	8
1.10.... Power Up Stone Lock® Pro	8
1.11.... Setting the Faceplate Address.....	8
1.12.... Installation Tables	9-11
1.13.... Connecting Stone Lock Pro to an Access Control System	12
1.14.... Voltage/Wire Gauge Tables ...	13-14

2.0 Using Stone Lock® Pro

2.01.... Startup Configurations	16
2.02.... Initial Enrollment.....	16
2.03.... Advanced Function Menu.....	18



3.0 User Management

3.01.... User Management Menu.....	20
3.02.... New User Enrollment Start	21
3.03.... Re-Enrollment Start	22
3.04.... Changing Cards.....	23
3.05.... Deleting A User	23
3.06.... Change User Type.....	24
3.07.... Check User Details	24



Section 4.0 Verification Records

4.01.... Verification Record Overview	26
4.02.... Verification Failures	26
4.03.... Record Viewing Date.....	27
4.04.... Viewing Previous Day's Records	27
4.05.... Viewing the Next Day's Records	28
4.06.... Viewing a Record's Details	28



5.0 Access Control

5.01.... Access Control Overview	30
5.02.... Device Permissions.....	30
5.03.... Door Settings.....	31
5.04.... Door Lock Settings	32
5.05.... Door Timer Setting	32
5.06.... Guest PIN Access	33
5.07.... Card # Parsing	34
5.08.... Door Sensor Settings.....	35
5.09.... Auxiliary Outputs & Inputs Overview	36
5.10.... Auxiliary Outputs.....	36
5.11.... Auxiliary Inputs	36
5.12.... Wiegand Configuration.....	38-39
5.13.... Silent Alarm	40



6.0 Network Functions

6.01.... Network Functions	42
6.02.... LAN	42
6.03.... Setting Up the IP Address	43
6.04.... Setting the Subnet Mask.....	43
6.05.... Setting the Gateway Address	44
6.06.... Setting the DNS Address	45
6.07.... IP Settings	45
6.08.... Web Service	46
6.09.... Real-Time Records.....	47
6.10.... Remote	48
6.11.... Auto Upload New User.....	48



7.0 System Settings

7.01.... System Settings.....	50
7.02.... Delete Users/Recs.....	50
7.03.... Security Level.....	51
7.04.... Alarm Settings	52
7.05.... Arm/Disarm Alarms.....	52
7.06.... SMS Module	53
7.07.... Event Linkage.....	55
7.08.... Aux In Linkage	55
7.09.... Wireless Linkage	56
7.10.... Impact Sensitivity.....	56
7.11.... Setting Verification Modes	57
7.12.... Setting Biometric Facial Recognition Only.....	58

7.0 System Settings (cont'd)

7.13.... Setting Biometric Facial Recognition with a Secondary Verification	59
7.14.... Setting Mixed Mode.....	60
7.15.... Setting Card Only.....	61
7.16.... Encrypting the User Information Upon Verification	61
7.17.... Setting User Interval	62
7.18.... Date/Time.....	62
7.19.... Time Settings.....	63
7.20.... Date Settings.....	63
7.21.... USB Operations.....	64
7.22.... Program Update.....	64
7.23.... Records Download.....	65
7.24.... User Download	65
7.25.... User Upload	66

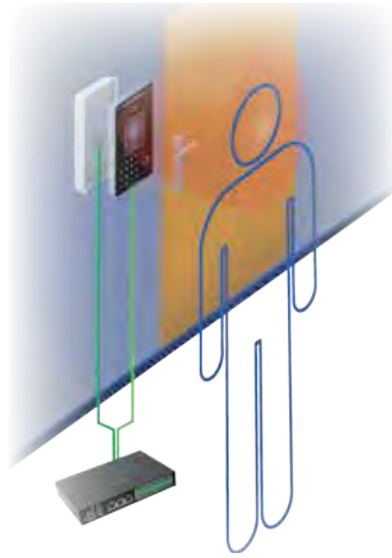


8.0 System Info

8.01.... System Info.....	68
---------------------------	----

9.0 Appendices

9.01.... Troubleshooting	70-77
9.02.... Product Specifications	78
9.03.... Dimension Drawings.....	79
9.04.... Warranty & Return Policy.....	80



Section 1: Introduction

1.01 Welcome to Stone Lock® Pro

1.02 Passive Interface

1.03 What's in the Box

1.04 Preparation for Installation

1.05 Locks

1.06 Stone Lock® Network Platform

1.07 Installation Checklist

1.08 Installation

1.09 Connecting Stone Lock® Pro

1.10 Power Up Stone Lock® Pro

1.11 Setting the Faceplate Address

1.12 Installation Tables – A, B, C

1.13 Voltage/Wire Gauge Tables



Stone Lock® Pro is a sophisticated biometric access control device that provides instant, reliable confirmation of identity

Section 1: Introduction

1.01 WELCOME TO STONE LOCK® PRO

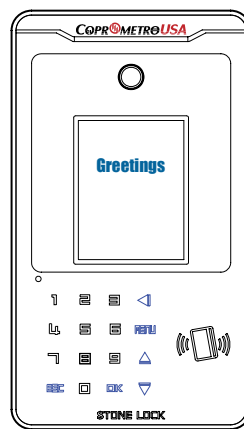
Congratulations on your purchase of Stone Lock® Pro! Stone Lock® Pro is an extremely accurate infrared biometric facial recognition device designed for access control applications. It is very reliable and easy to use.

Stone Lock® Pro is fast, accurate, safe, and simple. Stone Lock's proprietary hardware and software has been field proven as a reliable solution for the most critical access control applications.

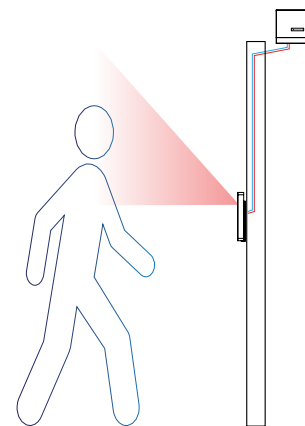
It is well suited for financial, medical, industrial, and other situations with critical security access demands.

Stone Lock® Passive Interface is designed for access verification with no contact and minimal effort on the part of the user. The user merely approaches facing the unit and it authenticates you instantly with a high level of convenience and assurance.

Stone Lock® Pro devices can be networked using the Stone Lock® Network Software. Stone Lock® Pro devices are also certified to a growing list of enterprise security platforms.



Stone Lock Pro® Device



Stone Lock Pro® Passive Interface

Stone Lock® Pro Features:

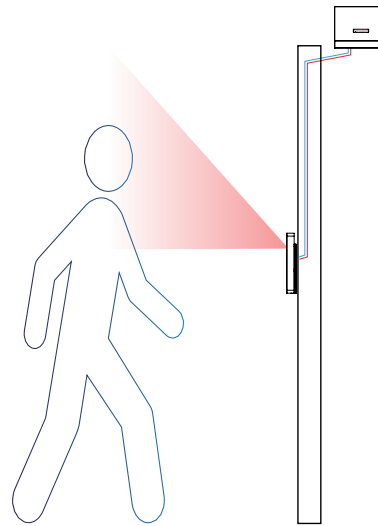
- ✓ Stone Lock® Pro's near-infrared biometric technology is ideal for access control, creating a safe, passive, even enjoyable user experience that is very simple to learn and use
- ✓ The Stone Lock® Passive Interface actuates instantly as a user approaches the unit
- ✓ Stone Lock® Pro scans a user multiple times a second, each time measuring over 2,000 points on the user's face
- ✓ Verification is Instant (<1 second)
- ✓ False Acceptance (FAR) exceeds = <0.0004%
- ✓ Multi-Factor Verification: Biometric, HID iClass SE Reader, Keypad
- ✓ RS485, Wiegand, USB, Cat5/5e/6 Ethernet
- ✓ Operates as a stand-alone or can be networked via a LAN
- ✓ Stone Lock® Network platform software supports groupings, scheduling, overrides, remote enrollment, permission management, other admin functions
- ✓ Stone Lock® Pro provides instant, consistent, and highly accurate verification

1.02 STONE LOCK® PASSIVE INTERFACE

The Stone Lock® Passive Interface allows a user to interact with a Stone Lock® Pro device with minimal effort. It is what makes Stone Lock® Pro so easy to learn and use.

Stone Lock® Passive Interface sensors scan the user's face with infrared wavelengths several times a second. The user doesn't touch anything; he or she merely approaches the Faceplate facing the unit, and Stone Lock® Pro actuates instantly when it senses someone within arms length of the unit. Stone Lock® Passive Interface has many advantages as an access control technology:

- Near-infrared wavelengths are safe, invisible to the eye, and relatively unaffected by ambient light or temperature
- Near-infrared is ideal for capturing intrinsic properties of a face (shape, reflectivity, and expression) while minimizing unfavorable characteristics of extrinsic factors (such as ambient illumination and misalignment)
- There is no known way to fake Stone Lock® Pro's proprietary technology into a false acceptance (i.e. simulate a near-infrared biometric measurement of a real person registered in the database)
- Stone Lock® Pro is safe, passive, simple, excels in convenience in almost every way, and appeals to a wide range of people of all ages, nationalities, and walks of life



Stone Lock Pro® Passive Interface
The Stone Lock® Passive Interface is designed to require almost no effort on the part a user.

Stone Lock® Pro Enhances Security in Your Critical Areas

- ✓ Real-time event capture
- ✓ Dual faceplate applications
- ✓ Live video stream ties back to your VMS
- ✓ ADA applications
- ✓ High-throughput areas
- ✓ Temporary access situations

For inquiries related to Stone Lock® Pro, contact sales@coprometrousa.com

SOFTWARE HOUSE
From Tyco Security Products



COPROMETROUSA® is an
HID Embedded Solutions Partner

1.03 WHAT'S IN THE BOX?

Stone Lock® Pro comes with installation hardware. A current Stone Lock® Pro Packing List (**Fig 1.03-1**) can be downloaded from www.stonelockpro.com/products.



Fig 1.03-1

a) The Faceplate

The Faceplate (**Fig 1.03-2**) is used to biometrically scan a user's face, display real-time interactive feedback, read card information, PIN numbers, control device functions, and communicate with the Control Unit.

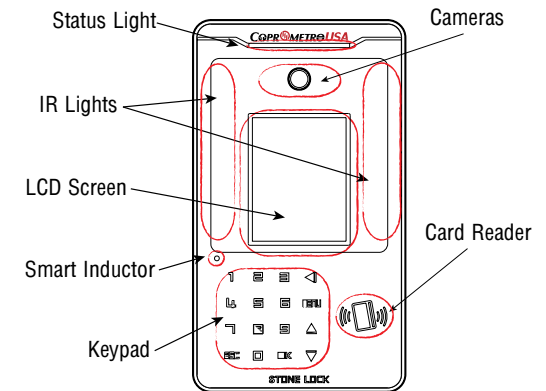


Fig 1.03-2

b) The Control Unit

The Control Unit (**Fig 1.03-3**) is the brain of the Stone Lock® Pro system.

It is used to receive, process and authenticate user information, send permissions, process and save information related to users, provide the output unlock signal and alarm signal via corresponding ports.

Additional I/O includes power, communication, network, USB, video extension, access ports.

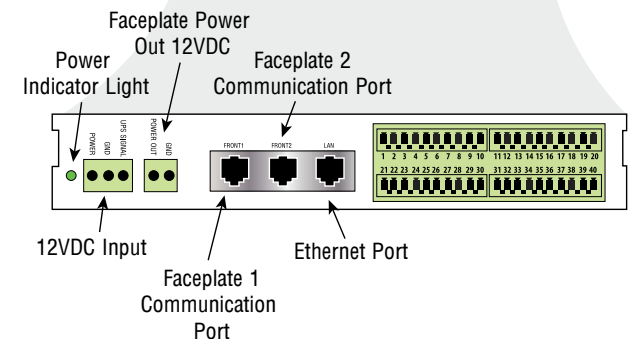
The Control Unit can be installed remotely (within 80 ft. / 25 m) from the Faceplate in a secure location.



Fig 1.03-3

(Control Unit Pin Out Ports)

Reference **Section 1.12** for a Complete Description of the Control Unit Pin Out Ports



1.04 PREPARATION FOR INSTALLATION

Power Supply and Wire Gauge Specifications:

Use Battery Backup System

It is highly recommended to power Stone Lock® Pro with a non-shared source that incorporates a battery backup system.

- a. A minimum of 18 AWG and a maximum of 12 AWG wire should be used for power between the faceplate and the control unit. The faceplate and control unit may be installed up to a maximum distance of 80 feet apart.
- b. Use the following steps to specify the proper power supply:
 - i. Determine if a battery backup is needed in the application
 - ii. If battery backup is needed in the application, determine if Stone Lock® Pro will be required to signal and record an alarm when switching to battery backup.
 - iii. If a battery backup alarm is needed, determine if it is desired to have the power supply provide a method for pulling the “UPS Signal” pin low on the control unit, or if Stone Lock® Pro is required to sense that it is running on battery backup because the input voltage has dropped below 13.0 VDC.
 - iv. Of the Stone Lock Pro hardware functions listed in **Fig 1.04-1** below, determine which ones will be used in the application.
 - v. Based on steps i-iv above, use the table **Fig 1.04-1** below to calculate how much current Stone Lock® Pro will require.

Stone Lock® Pro Functions/ Configurations	Current Draw WITH Battery Backup		Current Draw WITHOUT any Battery Backup (Table I Below) (Amps)	Total Current Draw (Amps)
	WITHOUT UPS Signal (Table II Below) (Amps)	WITH UPS Signal (Table I Below) (Amps)		
Facial Verification Only w/ 1 Faceplate	1.5	2.0	2.0	
Facial Verification Only w/ 2 Faceplates	2.0	2.5	2.5	
Stone Lock® Pro Powering Lock #1	2.0	2.0	2.0	
Stone Lock® Pro Powering Lock #2	2.0	2.0	2.0	
Stone Lock® Pro Powering Aux Output 1	2.0	2.0	2.0	
Stone Lock® Pro Powering Aux Output 2	2.0	2.0	2.0	
Using Auxiliary Power Output (Pins 19 & 20)	1.0	1.0	1.0	

Fig 1.04-1

1.05 LOCKS

Stone Lock® Pro is compatible with electric locks, magnetic locks and electric mortise locks – consult your integrator for specific hardware compatibility and installation.

1.06 THE STONE LOCK® NETWORK PLATFORM

The Stone Lock® Network (SLN) platform software is designed for installation on a centralized server. For a full description of all Stone Lock® Network functions download the Stone Lock® Network User Guide at www.stonelockpro.com/technical

Use **Table 1.04-1** along with the tables in **Section 1.13** to determine specific requirements for a dedicated adjustable DC Power Supply

Use the appropriate table in **Section 1.13** to calculate the proper power supply/wire gauge/wire length combination for your installation. Both tables indicate an approximate supply voltage setting based on using the maximum length for a specific gauge of wire at a specific current. Both tables also indicate the mV/ft voltage drop for each gauge of wire at a specific current.

1.07 INSTALLATION CHECKLIST

Please review the following checklist before moving on to installation (*See detailed steps at right*):

a) Stone Lock® Pro Specification Checklist

b) Check Voltage and Wire Gauge Requirements

c) Verify Faceplate Mounting Height

d) Verify the Ambient Lighting is Suitable for the Faceplate Location

Use Battery Backup System

It is highly recommended to power Stone Lock® Pro with a non-shared source that incorporates a battery backup system.
Reference Section 1.04.

For Indoor Use Only

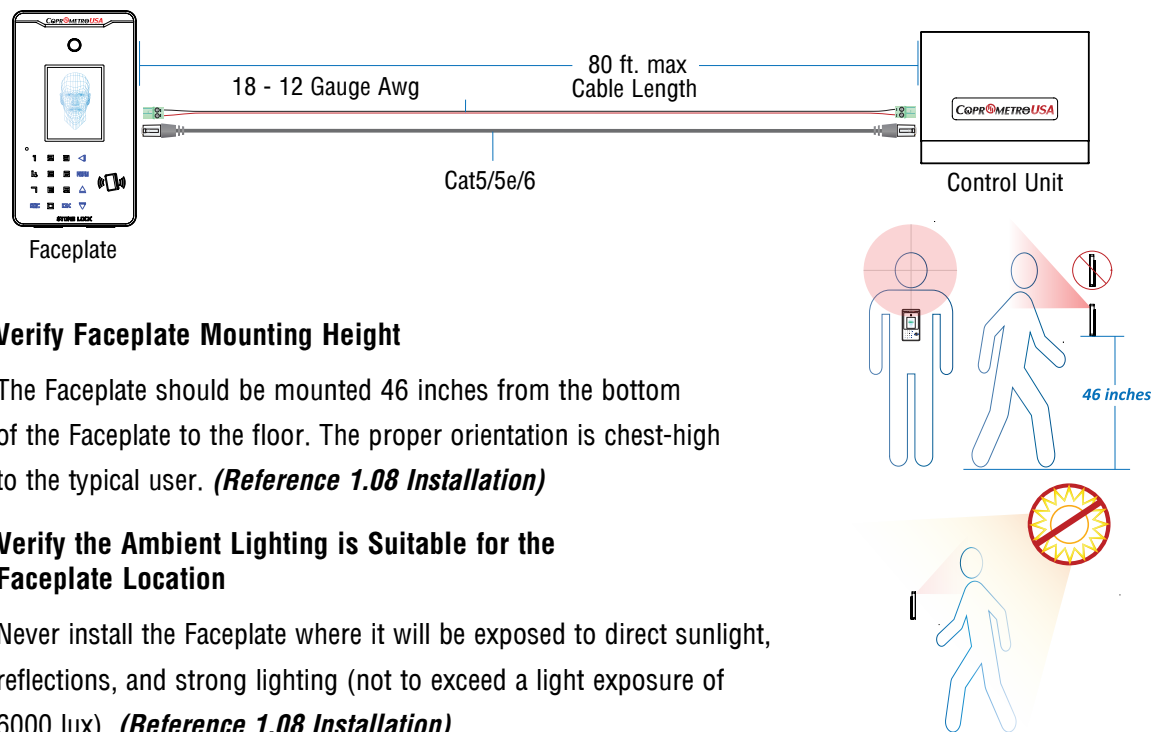
NOTE: Stone Lock® Pro is not recommended for outdoor use. Please contact sales@coprometrousa.com for special application information.

a) Stone Lock® Pro Specification Checklist

Did you, your integrator, or someone in your organization fill out a Stone Lock® Pro Hardware Configuration Sheet before ordering this unit? If so please review that document for any specific Sensor Inputs, Auxiliary I/O or other application requirements. *Download the Stone Lock® Pro Hardware Configuration Sheet at www.stonelockpro.com/technical.*

b) Check Voltage and Wire Gauge Requirements

- i. Confirm that the cable length between the Faceplate and the Control Unit is no more than 80 ft. in length, and a minimum of 18 AWG wire (max 12 Awg). **Reference 1.09 Connecting Stone Lock® Pro.**
- ii. Verify that the DC power supply voltage at the back of the Control Unit is between the limits shown in the relevant table in **Section 1.13** used to calculate wire gauge and the distance parameters **Reference 1.13 Power Supply and Wire Gauge Specifications (p.12).**



c) Verify Faceplate Mounting Height

The Faceplate should be mounted 46 inches from the bottom of the Faceplate to the floor. The proper orientation is chest-high to the typical user. (**Reference 1.08 Installation**)

d) Verify the Ambient Lighting is Suitable for the Faceplate Location

Never install the Faceplate where it will be exposed to direct sunlight, reflections, and strong lighting (not to exceed a light exposure of 6000 lux). (**Reference 1.08 Installation**)

1.08 INSTALLATION

When installing Stone Lock® Pro, Faceplate positioning is very important. The Stone Lock® Pro Faceplate should typically be mounted at a height of 46 inches from the bottom of the Faceplate to the floor, with the following considerations:

- The Faceplate should be chest-height to the user for best operation. (*Fig 1.08-2*)
- If the Faceplate is mounted too high, users below the camera range may experience trouble activating the unit. Users who fall outside the scan area may have problems activating the unit.
- Never install the Faceplate where it will be exposed to direct sunlight, reflections, and strong lighting (not to exceed a light exposure of 6000 lux).
- Before the installation of the Stone Lock® Pro unit, cables should be prepared and installed. All connectors required are included with Stone Lock® Pro, including 2 RJ45 connectors. Required cables and wirings include: Faceplate/Control Unit communication wire (recommended using Cat5/5e/6), and network communication cables.
- Maximum distance between Faceplate and Control Unit should be no more than 80ft. (<25 meters).

Installing the Faceplate:

Normally the faceplate is installed alongside the door. (*Fig 1.08-1*)

The Faceplate should typically be installed at a height of 46 inches from the floor to the bottom of the Faceplate. At a 46" height the Faceplate will detect users approximately 5 to 6.5 feet in height, and positions the keypad at a height commensurate with typical ADA requirements.

Installing the Control Unit:

The primary advantage of a separate Control Unit is that by mounting the Control Unit remotely, all the data and records processed at the Unit are not vulnerable to anything that might affect the Faceplate. In the event of vandalism or theft, since the Control Unit is installed on the secure side of the wall, the data, including a picture capture of the vandal caught in the act, is protected. (*Fig 1.08-3*)

The Control Unit cannot be mounted more than 80 feet (less than 25 meters) from the Faceplate. Doing so can degrade the communications between the Faceplate and the Control Unit to the point of operational failure.

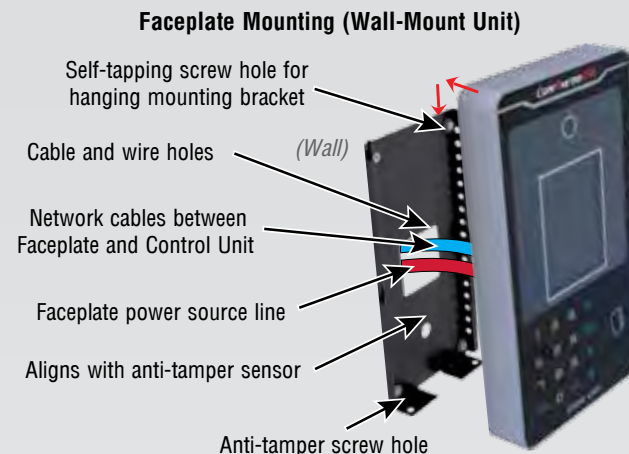


Fig 1.08-1

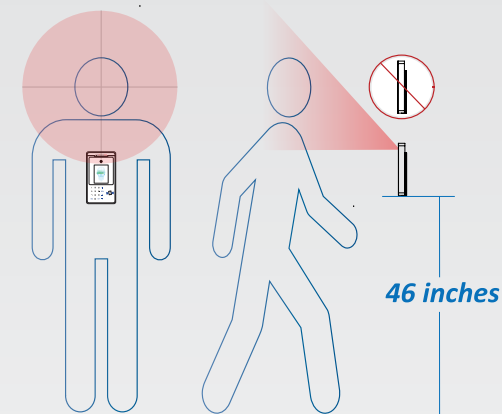


Fig 1.08-2

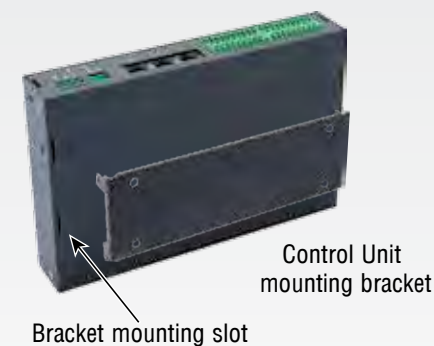


Fig 1.08-3

1.09 CONNECTING STONE LOCK® PRO

The fundamental connections between the Stone Lock® Faceplate and Control Unit involve a power cable and a communication cable, both of which plug into the front of the Control Unit and the back of the Faceplate.

Power is supplied to the Control Unit, and an Ethernet connection is available if you are hooking your Stone Lock® Pro up to a network. In addition, there are 40 additional pin-out connectors detailed in **Section 1.12**.

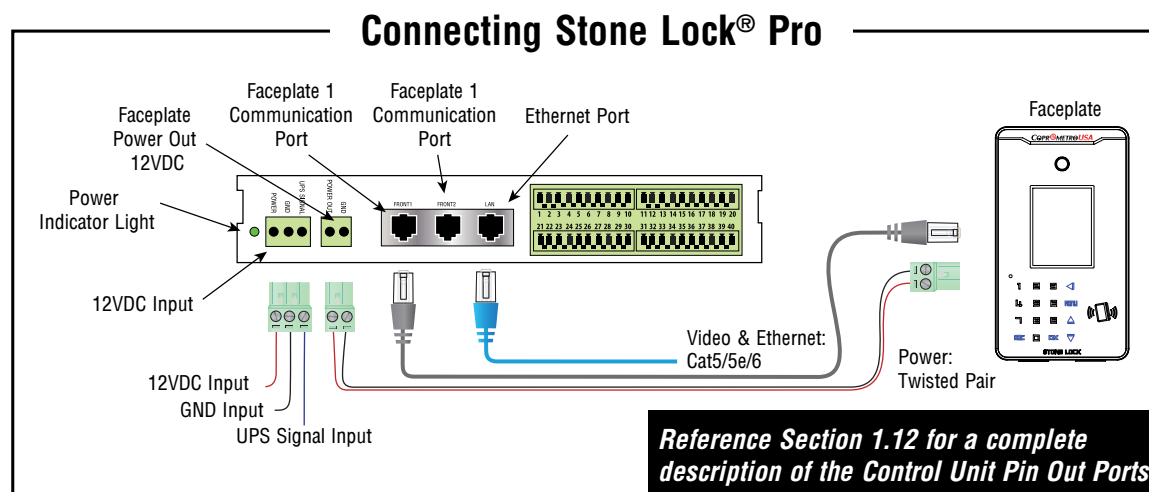
Note: For any Access Control System, please refer to diagram in **Section 1.13**.

1.10 READY TO POWER-UP STONE LOCK® PRO

Your Stone Lock® Pro device is installed and ready for power-up and initial user setup. Please continue on to Section 2 Using Stone Lock® Pro. For more information about Stone Lock® Pro visit our website at www.stonelockpro.com

1.11 SETTING THE FACEPLATE ADDRESS

When a faceplate is received from the factory, its address is set to “11” by default. If the application requires only a single faceplate, then the address is already properly set and this section can be skipped. However, if the application requires the use of two faceplates, use the following steps to set the faceplate addresses.



There are two dual faceplate applications:

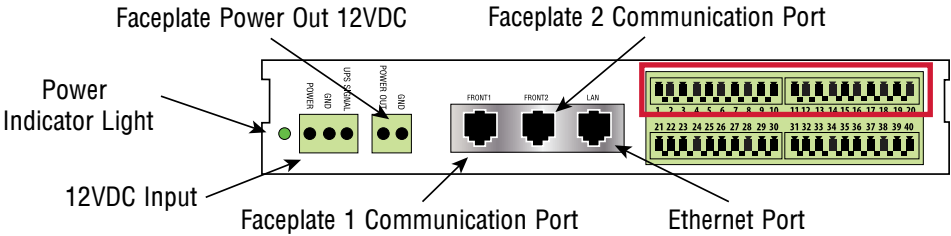
- One faceplate is used for entry and one faceplate is used for exit of the same access point. The faceplate used for entry should be connected to Front1 on the Control Unit. Its address should be set to “11” (the default address from the factory). The faceplate used for exit should be connected to Front2 on the Control Unit. Its address should be set to “10”.
- Two faceplates are used for access in a man trap application (one faceplate for each access point).

Note: This application can only be implemented when the Stone Lock® Control Unit is controlling the locks of the access points. The faceplate used for the first access point of the man trap should be connected to Front1 on the Control Unit. Its address should be set to “11” (the default address from the factory). The faceplate used for the second access point of the man trap should be connected to Front2 on the Control Unit. Its address should be set to “20”.

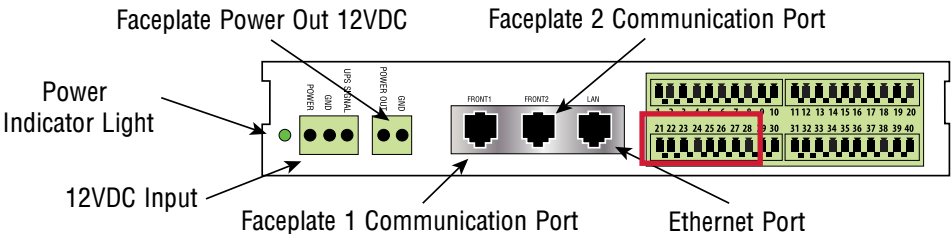
To set the faceplate address:

- Apply power to the Stone Lock® Pro system (Faceplates and Control Unit)
- Touch “0” on the faceplate and hold it until the faceplate beeps and the light at the top turns green.
- Release “0” and enter the appropriate address (11, 10 or 20 as described above).
- Touch “OK”.
- When the faceplate beeps and the light at the top turns white, the address was set successfully.

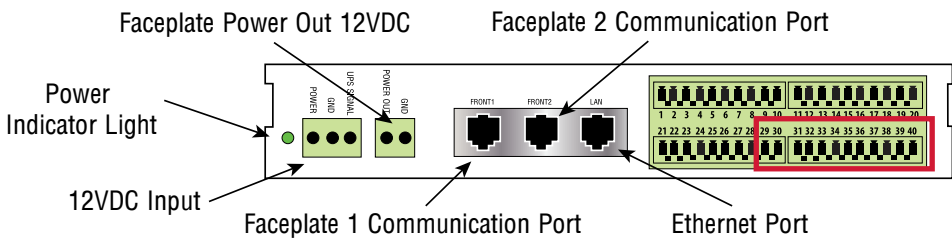
1.12 CONTROL UNIT PIN OUT PORT TABLE - A

Control Unit Pin Out Ports (1-20)			
			
Exit Door Open Button Input 1	1	Button1	Manually controls Electronic Lock Output 1 by pulling this TTL Input to Low (0 VDC) or connecting it to Ground.
	2	GND	Ground
Door Magnet Sensor Input 1	3	Sensor1	Senses that Door 1 is open when this TTL Input is NOT pulled Low (0 VDC) or NOT connected to Ground.
	4	GND	Ground
Exit Door Open Button Input 2	5	Button2	Manually controls Electronic Lock Output 2 by pulling this TTL Input to Low (0 VDC) or connecting it to Ground.
	6	GND	Ground
Door Magnet Sensor Input 2	7	Sensor2	Senses that Door 2 is open when this TTL Input is NOT pulled Low (0 VDC) or NOT connected to Ground.
	8	GND	Ground
Video Monitor Out	9	CCTV+	Standard PAL Video Output
	10	CCTV-	
Auxiliary Input 1	11	AUX1	TTL Input Port 1 that is configurable to detect either Low (0.0 VDC) to High (4.0 VDC) transitions or High to Low transitions. Can be pulled Low by connecting to Ground via a switch.
	12	GND	Ground
Auxiliary Input 2	13	AUX2	TTL Input Port 2 that is configurable to detect either Low (0.0 VDC) to High (4.0 VDC) transitions or High to Low transitions. Can be pulled Low by connecting to Ground via a switch.
	14	GND	Ground
Auxiliary Input 3	15	AUX3	TTL Input Port 3 that is configurable to detect either Low (0.0 VDC) to High (4.0 VDC) transitions or High to Low transitions. Can be pulled Low by connecting to Ground via a switch.
	16	GND	Ground
Auxiliary Input 4	17	AUX4	TTL Input Port 4 that is configurable to detect either Low (0.0 VDC) to High (4.0 VDC) transitions or High to Low transitions. Can be pulled Low by connecting to Ground via a switch.
	18	GND	Ground
Auxiliary Power Output	19	AUXP	Supplies 12 VDC / 1Amp Max for external equipment.
	20	GND	Ground

1.12 CONTROL UNIT PIN OUT PORT TABLE - B

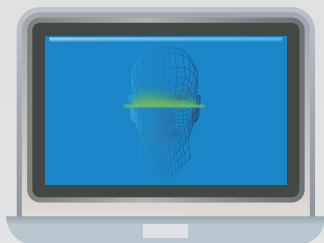
Control Unit Pin Out Ports (21-28)			
			
Electronic Lock Output 1	21	Close1	Passive Mode: Used as the Normally Closed Pin of a standard relay with the EPOW1 pin as the common. Connected to the EPOW1 pin until after successful user authentication when it is disconnected from the EPOW1 pin. After the “Door timer” time interval, it is reconnected to the EPOW1 pin. Active Mode: Supplies 12 VDC, until after successful user authentication. Then, no voltage is supplied until after the “Door timer” time interval when 12 VDC is supplied again. Electric Mode: Supplies a 5 VDC, 500ms pulse signal after successful user authentication.
	22	Open1	Passive Mode: Used as the Normally Open Pin of a standard relay with the EPOW1 pin as the common. Disconnected from the EPOW1 pin until after successful user authentication when it is connected to the EPOW1 pin. After the “Door timer” time interval, it is disconnected from the EPOW1 pin. Active Mode: No voltage is supplied, until after successful user authentication. Then, 12 VDC is supplied until after the “Door timer” time interval when no voltage is again supplied. Electric Mode: Supplies a 5 VDC, 500ms pulse signal after the “Door timer” time interval.
	23	EPOW1	Passive Mode: Used as the Common Pin of a standard relay. Connected to the Close1 pin until after successful user authentication when it is connected to the Open1 pin. After the “Door timer” time interval, it is disconnected from the Open 1 pin and reconnected to the Close 1 pin. Active Mode: Supplies a continuous 12 VDC signal. Electric Mode: Supplies a 5 VDC, 500ms pulse signal after successful user authentication followed by another 5 VDC, 500ms pulse signal after the “Door timer” time interval.
	24	GND	Ground
Electronic Lock Output 2	25	Close2	Passive Mode: Used as the Normally Closed Pin of a standard relay with the EPOW2 pin as the common. Connected to the EPOW2 pin until after successful user authentication when it is disconnected from the EPOW2 pin. After the “Door timer” time interval, it is reconnected to the EPOW2 pin. Active Mode: Supplies 12 VDC, until after successful user authentication. Then, no voltage is supplied until after the “Door timer” time interval when 12 VDC is supplied again. Electric Mode: Supplies a 5 VDC, 500ms pulse signal after successful user authentication.
	26	Open2	Passive Mode: Used as the Normally Open Pin of a standard relay with the EPOW2 pin as the common. Disconnected from the EPOW2 pin until after successful user authentication when it is connected to the EPOW2 pin. After the “Door timer” time interval, it is disconnected from the EPOW2 pin. Active Mode: No voltage is supplied, until after successful user authentication. Then, 12 VDC is supplied until after the “Door timer” time interval when no voltage is again supplied. Electric Mode: Supplies a 5 VDC, 500ms pulse signal after the “Door timer” time interval.
	27	EPOW2	Passive Mode: Used as the Common Pin of a standard relay. Connected to the Close2 pin until after successful user authentication when it is connected to the Open2 pin. After the “Door timer” time interval, it is disconnected from the Open 2 pin and reconnected to the Close 2 pin. Active Mode: Supplies a continuous 12 VDC signal. Electric Mode: Supplies a 5 VDC, 500ms pulse signal after successful user authentication followed by another 5 VDC, 500ms pulse signal after the “Door timer” time interval.
	28	GND	Ground

1.12 CONTROL UNIT PIN OUT PORT TABLE - C

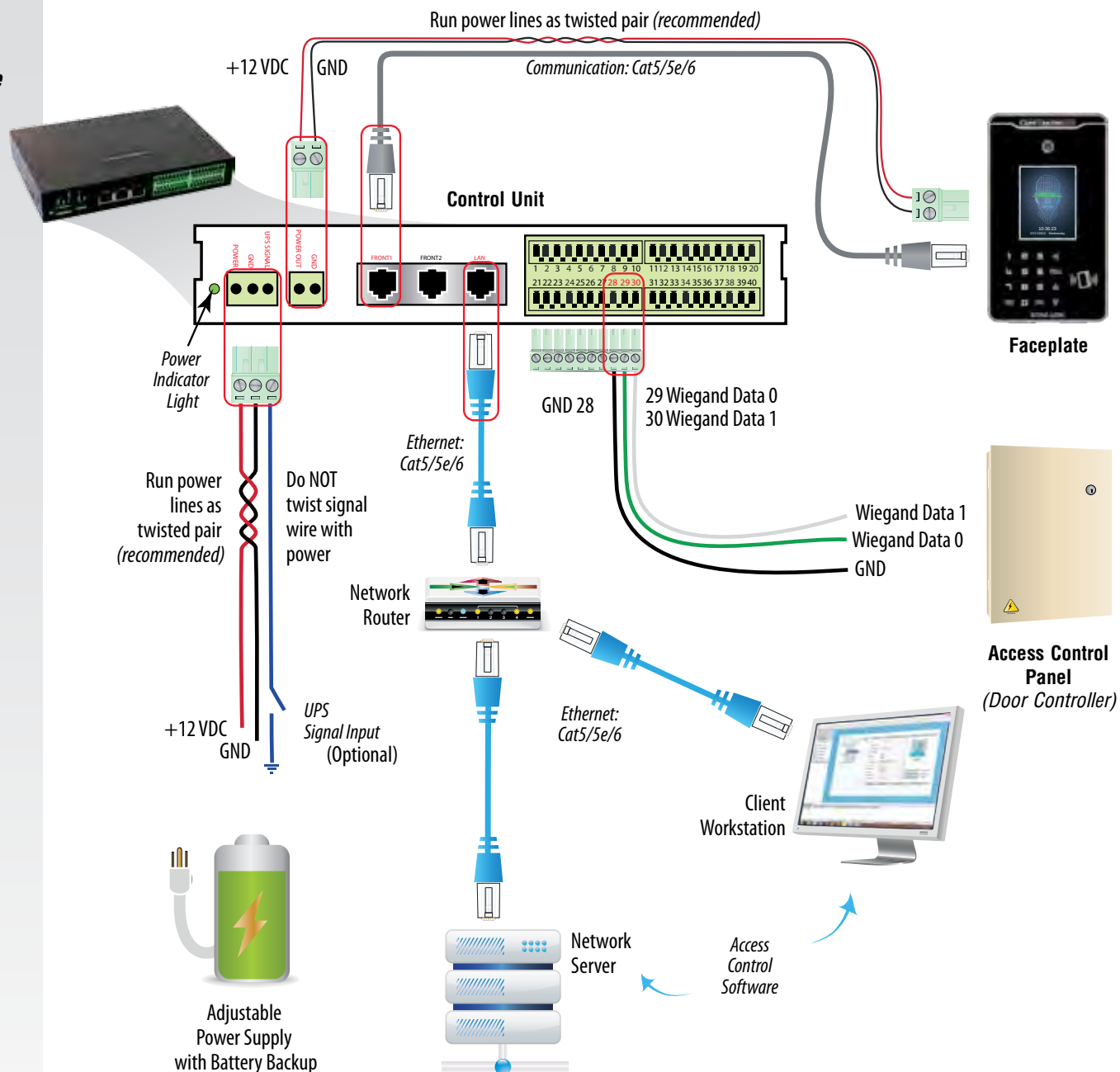
Control Unit Pin Out Ports (29-40)			
			
Wiegand Output	29	WGOUT0	Wiegand data 0
	30	WGOUT1	Wiegand data 1
Auxiliary Output 1	31	NC1	Passive Mode: Used as the Normally Closed Pin of a standard relay with the COM1 pin as the common. Connected to the COM1 until a designated alarm event. Is reconnected to COM1 6 seconds after the designated alarm event. Active Mode: Supplies 12 VDC until a designated alarm event. After the event, no voltage is supplied for 6 seconds and then 12 VDC is supplied again.
	32	NO1	Passive Mode: Used as the Normally Open Pin of a standard relay with the COM1 pin as the common. Disconnected from the COM1 until a designated alarm event. Then is connected to COM1 for 6 seconds and then disconnected again. Active Mode: No voltage is supplied until a designated alarm event. After the event, 12 VDC is supplied for 6 seconds and then no voltage is supplied again.
	33	COM1	Passive Mode: Used as the Common Pin of a standard relay. Connected to the NC1 pin until a designated alarm event. Connected to NO1 pin for 6 seconds and then reconnected to NC1. Active Mode: Supplies a continuous 12 VDC signal.
	34	GND	Ground
Auxiliary Output 2	35	NC2	Passive Mode: Used as the Normally Closed Pin of a standard relay with the COM2 pin as the common. Connected to the COM2 until a designated alarm event. Is reconnected to COM2 6 seconds after the designated alarm event. Active Mode: Supplies 12 VDC until a designated alarm event. After the event, no voltage is supplied for 6 seconds and then 12 VDC is supplied again.
	36	NO2	Passive Mode: Used as the Normally Open Pin of a standard relay with the COM2 pin as the common. Disconnected from the COM2 until a designated alarm event. Then is connected to COM2 for 6 seconds and then disconnected again. Active Mode: No voltage is supplied until a designated alarm event. After the event, 12 VDC is supplied for 6 seconds and then no voltage is supplied again.
	37	COM2	Passive Mode: Used as the Common Pin of a standard relay. Connected to the NC2 pin until a designated alarm event. Connected to NO2 pin for 6 seconds and then reconnected to NC2. Active Mode: Supplies a continuous 12 VDC signal.
	38	GND	Ground
RS485 (In/Out)	39	RS485A	RS-485 communication wire A (D +) port
	40	RS485B	RS-485 communication wire A (D -) port

1.13 CONNECTING STONE LOCK PRO TO AN ACCESS CONTROL SYSTEM

See [next] **Section 1.14 Voltage/Wire Gauge Tables** for more information on wiring.



NOTE: Make sure that you have installed appropriate drivers and software to allow Stone Lock® Pro to operate with your Access Control System. Consult your integrator for details.



1.14 VOLTAGE / WIRE GAUGE TABLES

Table I. Based on the calculated total current draw of the unit, use Table I to determine the maximum distance and wire gauge if one of the following conditions exist: (a.) A power supply is used with a battery backup and has the ability to pull the “UPS Signal” pin low, or (b.) A power supply is used without a battery backup

Maximum Power Supply Wire Length Table I																				
Either: WITH a Battery Backup AND WITH a UPS Signal or WITHOUT a Battery Backup																				
(Assumes the voltage at the unit is set between 10.3 and 12.9 VDC during verification)																				
Supply Current (A)	2	2.5	3	3.5	4	4.5	5	5.5	6	6.5	7	7.5	8	8.5	9	9.5	10	10.5	11	11.5
Supply Voltage (V)	12.9	12.9	12.9	12.9	12.9	12.9	12.9	12.9	12.9	12.9	12.9	12.9	12.9	12.9	12.9	12.9	12.9	12.9	12.9	12.9
Wire Gauge	12	409ft 6.35	327ft 7.94	272ft 9.53	233ft 11.12	204ft 12.71	181ft 14.29	163ft 15.88	148ft 17.47	136ft 19.06	125ft 20.65	116ft 22.24	109ft 23.82	102ft 25.41	96ft 27.00	90ft 28.59	86ft 30.18	81ft 31.77	77ft 33.35	74ft 34.94
	14	257ft 10.10	205ft 12.63	171ft 15.15	147ft 17.68	128ft 20.20	114ft 22.73	102ft 25.26	93ft 27.78	85ft 30.31	79ft 32.83	73ft 35.36	68ft 37.88	64ft 40.41	60ft 42.93	57ft 45.46	54ft 47.99	51ft 50.51	49ft 53.04	46ft 55.56
	16	161ft 16.06	129ft 20.07	107ft 24.09	92ft 28.10	80ft 32.11	71ft 36.13	64ft 40.14	58ft 44.16	53ft 48.17	49ft 52.18	46ft 56.20	43ft 60.21	40ft 64.23	38ft 68.24	35ft 72.26	34ft 76.27	32ft 80.28		
	18	101ft 25.54	81ft 31.93	67ft 38.31	58ft 44.70	50ft 51.08	45ft 57.47	40ft 63.86	37ft 70.24	33ft 76.63										
	20	64ft 40.61	51ft 50.76	42ft 60.92	36ft 71.07	32ft 81.22														
	22	40ft 64.57																		
Voltage Drop (mv/ft)																				

Table II. Based on the calculated total current draw of the unit, use Table II to determine maximum distance and wire gauge if a power supply is used with a battery backup but without the ability to pull the “UPS Signal” pin low.

Maximum Power Supply Wire Length Table II																				
WITH Battery Backup BUT WITHOUT a UPS Signal																				
(Assumes the voltage at the unit is set between 13.2 and 13.8 VDC during verification)																				
Supply Current (A)	1.5	2	2.5	3	3.5	4	4.5	5	5.5	6	6.5	7	7.5	8	8.5	9	9.5	10	10.5	11
Supply Voltage (V)	14.11	14.19	13.95	14.01	13.90	13.95	13.88	13.91	13.86	13.89	13.85	13.88	13.84	13.87	13.84	13.86	13.83	13.85	13.83	13.85
Wire Gauge	12	190ft 4.76	155ft 6.35	94ft 7.94	85ft 9.53	63ft 11.12	58ft 12.71	47ft 14.29	44ft 15.88	37ft 17.47	36ft 19.06	31ft 20.65	30ft 22.24	27ft 23.82	26ft 25.41	23ft 27.00	22ft 28.59	21ft 30.18	20ft 31.77	18ft 33.35
	14	119ft 7.58	97ft 10.10	59ft 12.63	53ft 15.15	39ft 17.68	36ft 20.20	29ft 22.73	28ft 25.26	23ft 27.78	22ft 30.31	19ft 32.83	19ft 35.36	16ft 37.88	16ft 40.41	14ft 42.93	14ft 45.46	13ft 47.99	12ft 50.51	11ft 53.04
	16	75ft 12.04	61ft 16.06	37ft 20.07	33ft 24.09	24ft 28.10	23ft 32.11	18ft 36.13	18ft 40.14	14ft 44.16	14ft 48.17	12ft 52.18	12ft 56.20	10ft 60.21	10ft 64.23	9ft 68.24	9ft 72.26	8ft 76.27	8ft 80.28	
	18	47ft 19.16	38ft 25.54	23ft 31.93	21ft 38.31	15ft 44.70	14ft 51.08	11ft 57.47	11ft 63.86	9ft 70.24	9ft 76.63									
	20	29ft 30.46	24ft 40.61	14ft 50.76	13ft 60.92	9ft 71.07	9ft 81.22													
	22	18ft 48.43																		
Voltage Drop (mv/ft)																				

Both of these tables indicate an approximate supply voltage setting based on using the maximum length for a specific gauge of wire at a specific current.

Both tables also indicate the mV/ft voltage drop for each gauge of wire at a specific current.

How to Use The Tables:

If your Power Supply...		
has a Backup Battery with...		...does not have a Backup Battery
...NO UPS Signal	...UPS Signal pulls UPS PIN low	
Table II	Table I	Table I

Both of these tables indicate an approximate supply voltage setting based on using the maximum length for a specific gauge of wire at a specific current.

Both tables also indicate the mV/ft voltage drop for each gauge of wire at a specific current.

See also **Actual Wire Gauge Table (Table III)** on next page.

Recommended Voltage Level

NOTE: Typically, a 3% or less drop in voltage from the supply to the unit is the recommended level for efficient operation of Stone Lock® Pro.

Notes:

1.14 VOLTAGE / WIRE GAUGE TABLES (CONT'D)

Table III. If wire is already installed, the table at the right can be used as a reference to combine wires in order to achieve an equivalent wire gauge.

Actual Wire Gauge												
Equivalent Wire Gauge		24	23	22	21	20	19	18	17	16	15	14
	12	16	13	11	9	7	6	5	4	3		2
	13	13	11	9	7	6	5	4	3		2	
	14	11	9	7	6	5	4	3		2		
	15	9	7	6	5	4	3		2			
	16	7	6	5	4	3		2				
	17	6	5	4	3		2					
	18	5	4	3		2						
	19	4	3		2							
	20	3		2								
	21		2									
	22	2										

Example: An 12 AWG is the same as using two (2) 14 AWG wires or sixteen (16) 24 AWG wires.

Example: An 12 AWG is the same as using two (2) 14 AWG wires or sixteen (16) 24 AWG wires.

Section 2: Using Stone Lock® Pro

2.01 Startup Configurations

2.02 Initial Enrollment

2.03 Advanced Function Menu



Section 2: Using Stone Lock® Pro

2.01 STARTUP CONFIGURATIONS

Stone Lock® Pro user types are divided into: S-Admin, Admin, User. As one would expect, different user types have different levels of privileges to perform operations related to users and devices.

User Type Privileges	
	S-Admin Has access to: all items in “Advanced Settings” menu. User privileges: can perform all operations except delete himself and change his type. Designated by a red user icon.
	Admin Has access to: user management, record inquiry, and system information. User privileges: add users, delete users, re-enroll users including himself; cannot perform any modifications to S-Admin profiles admin profiles, and cannot change any user types. Designated by an orange user icon.
	User Has NO access to the Advanced Setting menu. User privileges: Device activation privileges as defined by Admins. Designated by a blue user icon.

2.02 INITIAL ENROLLMENT

Preparation for Initial Enrollment

S-Admin

Stone Lock® Pro requires an S-Admin to access all menu functions, including new user enrollment. It is therefore HIGHLY recommended that at least TWO ACCESSIBLE PEOPLE be enrolled as an S-Admin to avoid being locked out of the menus. It is also important that if a 1:1 mode will be used, i.e. card + face that all S-Admins be enrolled with their card at initial enrollment and must remember their ID #.

Alignment

User should enroll with a non-expressive face that is easily replicated for daily access. The enrolling user should keep their face centered in the screen ensuring it is visible at all times and they should see the green scan bar on their face during enrollment. If at any time the scan bar is not seen on the image, the enrollment process has stalled and they are not being enrolled. If the enrollment process stalls more than once, touch **ESC**, educate the enrollee on proper technique, and restart the enrollment process again.

While enrolling, the user should SLIGHTLY (10-15° either direction) and slowly nod head side to side and up and down as the file builds.

Card ID

If you do not associate a card or ID # with a user record at the time of enrollment, you cannot do so at a later date and must re-enroll the user to associate 1:1 credentials.

***Glasses**

Stone Lock Pro enables the user to be verified with or without their glasses. If the user wears glasses, they should put them on at the beginning of the enrollment process. When the profile is about 50% complete (approximately 8 seconds into the enrollment process) and the message “Please Note: remove your glasses” appears, the user should quickly remove their glasses.

NOTE: Extremely thick lenses, safety glasses, sun glasses or dark transitional glasses may disrupt the scanning process and may have to be removed in order to use Stone Lock® Pro.

Initial Enrollment, S-Admin

The initial user to be enrolled on a Stone Lock® Pro device is enrolled as an S-Admin, granting the initial user the highest level of privileges to control all functions within the Stone Lock® Pro device.

Subsequent enrollments enter as ordinary users and must be upgraded by the S-Admin if other privilege levels are required. It is permissible to have multiple S-Admins.

a) When you power up Stone Lock® Pro, the device goes through an initial boot sequence. Wait until you see the animation start to cycle. **(Fig. 2.02-1)**

b) Touch **MENU** on the keypad to interrupt the Animation Cycles and initiate the New User screen. **(Fig. 2.02-2)**

c) Use the keypad to input a user ID# (1-18 digits). If you also want a card associated with this record, present the card at this point and listen for a chirp from the device. The card number will appear in the card line. **(Fig 2.02-3)**

- d) Touch **OK** to begin the enrollment process. The process should take about 15 seconds.
- e) The user should enroll with a non-expressive face that is easily replicated for daily access. The enrolling user should keep their face centered in the screen ensuring it is visible at all times and they should see the green scan bar on their face during enrollment.
- f) After enrollment is complete, the Advanced Settings menu will appear. From this menu, all local Stone Lock® Pro operations can be performed.
- g) Touch **ESC** on the keypad twice to exit the menu system and return to the Animation Cycle.

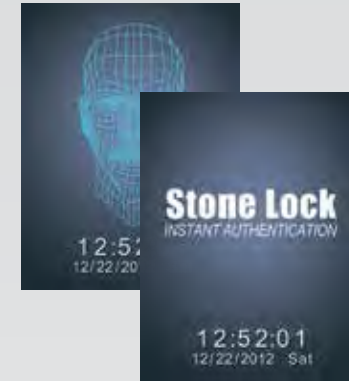


Fig 2.02-1

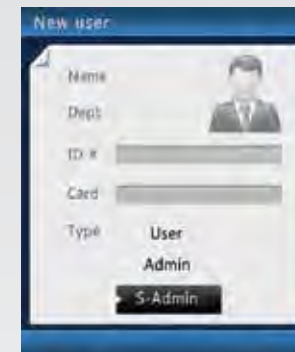


Fig 2.02-2

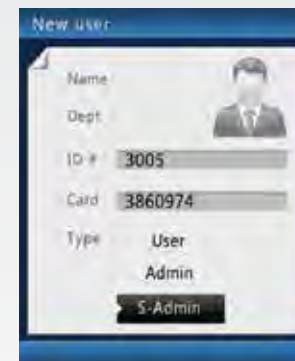


Fig 2.02-3



Fig 2.03-1



Fig 2.03-2



Fig 2.03-3

Troubleshooting: Green Scan Bar Is Not Seen

If at any time the green scan bar is not seen on the enrollment screen, this indicates enrollment has momentarily stalled, probably because the user is slightly out of range, has his/her head tilted or facial features are being blocked. Moving the user closer, straightening the user's posture, and removing obstacles respectively should resume the enrollment process.

2.03 ACCESS OF ADVANCED FUNCTION MENU

- As an S-Admin or Admin, at the Animation Cycle, touch **MENU**. The words "Administrator Authentication" (**Fig 2.03-1**) will be displayed at the top of the screen when verifying for device access.
- Using the same (non-expressive) face that was used during enrollment, the user should keep their face centered in the green frame of the verification screen.
- If the verification fails, a failure note will pop up (**Fig 2.03-2**), otherwise a success note (**Fig 2.03-3**), and the device will enter the Advanced Setting menu.

NOTE: If the verification mode is set to 1:1, the user must present a card or an ID # as described in 7.13 for proper verification.

Section 3: User Management



- 3.01 User Management Menu**
- 3.02 New User Enrollment Start**
- 3.03 Re-Enrollment**
- 3.04 Changing Cards**
- 3.05 Deleting A User**
- 3.06 Change User Type**
- 3.07 Check User Details**

Section 3: User Management

3.01 USER MANAGEMENT MENU

- a) As an enrolled S-Admin, access the Advanced Settings menu by touching **MENU** on the keypad and verifying with the device.
- b) From the Advanced Settings menu use the ▲ or ▼ keys to highlight the User Mgmt menu option. Touch **OK** to enter the menu.
- c) The User Mgmt menu defaults to all users being displayed in the user list. Users that are enrolled are indicated with a green dot next to the user icon. (Fig 3.01-1)



Fig 3.01- 1

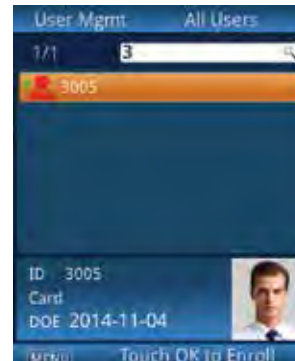


Fig 3.01- 2

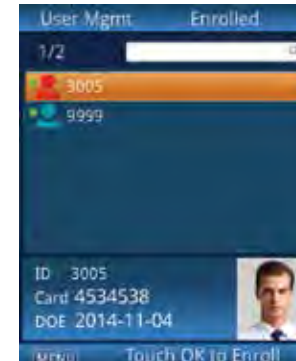


Fig 3.01- 3



Fig 3.01- 4

Touch any number key to search for users whose ID# begins with that number. For example, when the “3” key is pressed, the system automatically filters, and displays only those users whose ID# starts with “3”. (Fig 3.01-2)

d) To display all the users in the User Mgmt menu, touch **MENU** to show the menu selections. Use the ▲ or ▼ keys to highlight the All Users option and touch **OK**. (Fig 3.01-1)

e) To display in the User Mgmt menu only the users that are enrolled, touch **MENU** to pop up menu selections. Use the ▲ or ▼ keys to highlight the Enrolled option and then touch **OK**. (Fig 3.01-3)

f) To display in the User Mgmt menu only the users that have NOT been enrolled, Touch **MENU** to pop up menu selections. Use the ▲ or ▼ keys to highlight the No BSD option and then touch **OK**. (Fig 3.01-4)

Note: This function only exists when a profile has been pushed from a fully integrated access control system or the SLN, but the user has not been enrolled.

g) Touch **ESC** as necessary to exit all the menus.

3.02 NEW USER ENROLLMENT START

User Enrollment:

- As an enrolled S-Admin, access the Advanced Settings menu by touching **MENU** on the keypad and verifying with the device.
- From the Advanced Settings menu use the **▲** or **▼** keys to highlight the User Mgmt menu option. Touch **OK** to enter the menu. (Fig. 3.02-1)
- Touch the number keys to input the user ID# (4-18 digits). (Fig. 3.02-2)

Note: It is recommended to use at least a 4 digit ID number as you can't enter numbers of lesser value from where you have started, i.e. if you have a users with 1234, you will not be able to have a 1, a 12, or a 123.

- If the user is also to be enrolled with a card, present the card over the card symbol on the faceplate. The card number will be displayed in the User Mgmt menu. (Fig. 3.02-2)

- Touch **OK** to begin the enrollment process or touch **ESC** to discontinue the process and return to the User Mgmt menu.
- When the enrollment is successful, the "Registration Successful" screen with the ID #, the person's first and last name, the department and the time of enrollment will momentarily appear. (Fig. 3.02-3)
- The system automatically returns to the User Mgmt menu.
- Touch **ESC** as necessary to exit all the menus.

Note: The person's first and last name and the department will only appear if the profile was pushed from the Stone Lock® Network or from a fully integrated access control system.

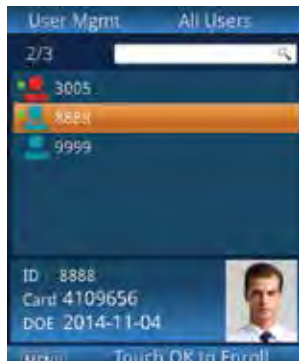


Fig 3.02-1

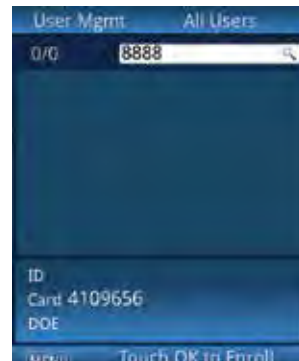


Fig 3.02-2



Fig 3.02-3

Preparation for User Enrollment:

Alignment

User should enroll with a non-expressive face that is easily replicated for daily access. The enrolling user should keep their face centered in the screen ensuring it is visible at all times and they should see the green scan bar on their face during enrollment. If at anytime the scan bar is not seen on the image, the enrollment process has stalled and they are not being enrolled. If the enrollment process stalls more than once, touch **ESC**, educate the enrollee on proper technique, and restart the enrollment process again.

While enrolling, the user should SLIGHTLY (10-15° either direction) and slowly nod head side to side and up and down as the file builds.

Glasses

Stone Lock® Pro enables the user to be verified with or without their glasses. If the user wears glasses, they should put them on at the beginning of the enrollment process. When the profile is about 50% complete (approximately 8 seconds into the enrollment process) and the message "Please Note: remove your glasses" appears, the user should quickly remove their glasses.

When the message "Please Note: Remove your glasses" appears at the bottom of the screen, please do so. (Fig 3.02-4)

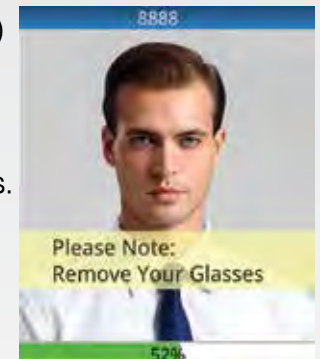


Fig 3.02-4

NOTE: Extremely thick lenses, safety glasses, sun glasses or dark transitional glasses may disrupt the scanning process and may have to be removed in order to use Stone Lock® Pro.

Preparation for User Enrollment:

Alignment

User should enroll with a non-expressive face that is easily replicated for daily access. The enrolling user should keep their face centered in the screen ensuring it is visible at all times and they should see the green scan bar on their face during enrollment. If at anytime the scan bar is not seen on the image, the enrollment process has stalled and they are not being enrolled. If the enrollment process stalls more than once, touch **ESC**, educate the enrollee on proper technique, and restart the enrollment process again.

While enrolling, the user should SLIGHTLY (10-15° either direction) and slowly nod head side to side and up and down as the file builds.

Glasses

Stone Lock® Pro enables the user to be verified with or without their glasses. If the user wears glasses, they should put them on at the beginning of the enrollment process. When the profile is about 50% complete (approximately 8 seconds into the enrollment process) and the message “Please Note: remove your glasses” appears, the user should quickly remove their glasses.

NOTE: Extremely thick lenses, safety glasses, sun glasses or dark transitional glasses may disrupt the scanning process and may have to be removed in order to use Stone Lock® Pro.

3.03 RE-ENROLLMENT

- As an enrolled S-Admin, access the Advanced Settings menu by touching **MENU** on the keypad and verifying with the device.
- From the Advanced Settings menu use the **▲** or **▼** keys to highlight the User Mgmt menu option. Touch **OK** to enter the menu.
- Select the user that needs to re-enroll by using the **▲** or **▼** keys to search the list or by entering the ID# of the user. (Fig.3.03-1)

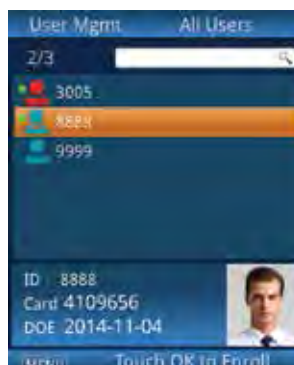


Fig 3.03-1

- If the user is also to be enrolled with a card, present the card over the card symbol on the faceplate. The card number will be displayed in the User Mgmt menu.
 - Touch **OK** to pop-up the re-enrollment dialog box.
 - Touch **OK** to begin the enrollment process or touch **ESC** to discontinue the process and return to the User Mgmt menu.
 - When the enrollment is successful, the “Registration” screen with the ID #, the person’s first and last name, the department and the time of enrollment will momentarily appear.
- Note:** The person’s first and last name and the department will only appear if the profile was pushed from the Stone Lock® Network or from a fully integrated access control system.
- The system automatically returns to the User Mgmt menu.
 - Touch **ESC** as necessary to exit all the menus.

3.04 CHANGING CARDS

- As an enrolled S-Admin, access the Advanced Settings menu by touching **MENU** on the keypad and verifying with the device.
- From the Advanced Settings menu use the **▲** or **▼** keys to highlight the User Mgmt menu option. Touch **OK** to enter the menu.
- Select the user that will be assigned to the card by using the **▲** or **▼** keys to search the list or by entering the ID# of the user. (**Fig 3.04-1**)
- Present the card over the card symbol on the face of the device. The card number will be displayed in the User Mgmt menu.
- If the user was previously assigned to a different card, then presenting the new card will cause a pop up dialogue box to appear asking to replace the old card number with the new card number. (**Fig 3.04-2**) Touch **OK** to confirm the new card number or touch **ESC** to discontinue the process and return to the User Mgmt menu. The new card number will be displayed in the User Mgmt menu.
- If you confirmed the new card, touch **OK** to re-enroll the user.
- Touch **ESC** as necessary to exit all the menus.

NOTE: Each card can only be registered to one user profile.

3.05 DELETING A USER

- As an enrolled S-Admin, access the Advanced Settings menu by touching **MENU** on the keypad and verifying with the device.
- From the Advanced Settings menu use the **▲** or **▼** keys to highlight the User Mgmt menu option. Touch **OK** to enter the menu.
- Select the user that is to be deleted by using the **▲** or **▼** keys to search the list or by entering the ID# of the user. (**Fig 3.05-1**)
- Touch **MENU** to pop up menu selections. Use the **▲** or **▼** keys to highlight the Delete option and then touch **OK**. (**Fig 3.05-2**)
- Touch **OK** to pop-up the delete confirmation dialog box. (**Fig 3.05-3**) Touch **OK** to delete the user and or touch **ESC** to discontinue the process and return to the User Mgmt menu.
- When the user has been deleted, the “Deleted Successfully” screen will momentarily appear (**Fig 3.05-4**)
- Touch **ESC** as necessary to exit all the menus.

NOTE: S-Admin cannot delete their own profile(s).

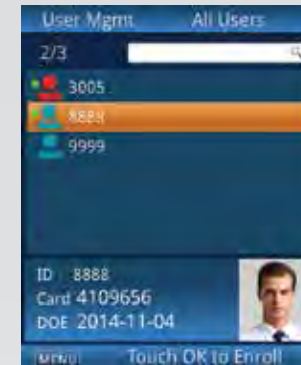


Fig 3.04-1

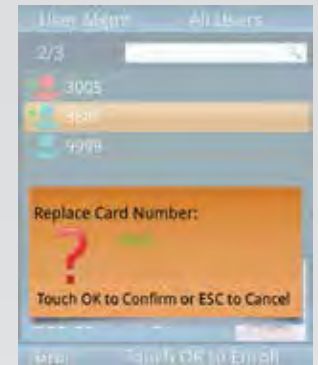


Fig 3.04-2



Fig 3.05-1

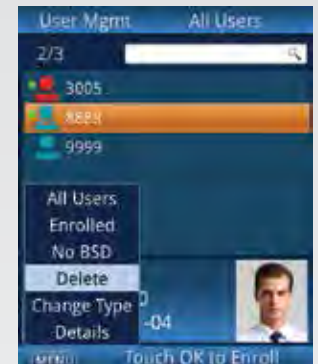


Fig 3.05-3

Fig 3.05-2

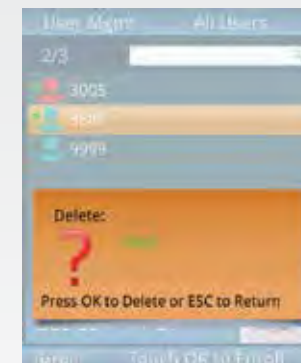


Fig 3.05-3



Fig 3.05-4

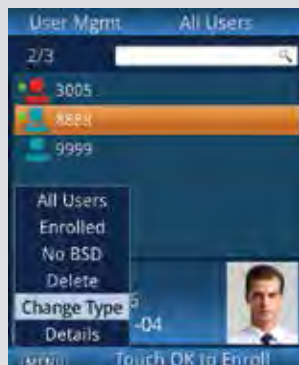


Fig 3.06-1



Fig 3.06-2

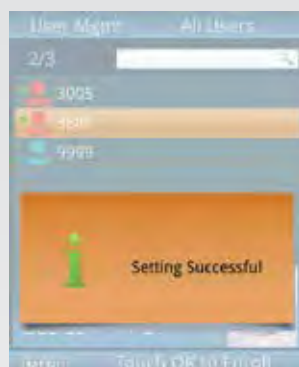


Fig 3.06-3

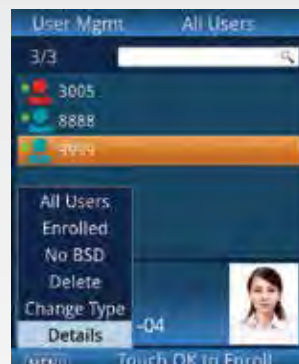


Fig 3.07-1

3.06 CHANGE USER TYPE

- As an enrolled S-Admin, access the Advanced Settings menu by touching **MENU** on the keypad and verifying with the device.
- From then Advanced Settings menu use the **▲** or **▼** keys to highlight the User Mgmt menu option. Touch **OK** to enter the menu.
- Select the user whose type needs to be modified by using the **▲** or **▼** keys to search the list or by entering the ID# of the user.
- Touch **MENU** to pop up menu selections. Use the **▲** or **▼** keys to highlight the Change Type option and then touch **OK**. (**Fig 3.06-1**)
- Use the **▲** or **▼** keys to highlight the desired privilege type, "User" "Admin" or "S-Admin". (**Fig 3.06-2**)
- Touch **OK** to accept the selected privilege or touch **ESC** to discontinue the process and return to the User Mgmt menu.
- When the user's privilege has been changed, the "Setting Successful" screen will momentarily appear. (**Fig 3.06-3**)
- Touch **ESC** as necessary to exit all the menus.

3.07 CHECK USER DETAILS

- As an enrolled S-Admin, access the Advanced Settings menu by touching **MENU** on the keypad and verifying with the device.
- From the Advanced Settings menu use the **▲** or **▼** keys to highlight the User Mgmt menu option. Touch **OK** to enter the menu.
- Select the user whose profile details need to be viewed by using the **▲** or **▼** keys to search the list or by entering the ID# of the user.
- Touch **MENU** to pop up menu selections. Use the **▲** or **▼** keys to highlight the Details option, and then touch **OK**. (**Fig 3.07-1**)
- The "Details" screen for the selected user will appear.
- Touch **ESC** to return to the User Mgmt menu.
- Touch **ESC** as necessary to exit all the menus.

Section 4: Verification Records



- 4.01 Verification Record Overview**
- 4.02 Verification Failures**
- 4.03 Record Viewing Date**
- 4.04 Viewing Previous Day's Records**
- 4.05 Viewing the Next Day's Records**
- 4.06 Viewing a Record's Details**

Section 4: Verification Records



Fig 4.01-1

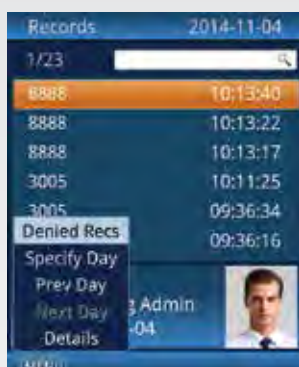


Fig 4.02-1

4.01 VERIFICATION OVERVIEW

- As an enrolled S-Admin, access the Advanced Settings menu by touching **MENU** on the keypad and verifying with the device.
- From the Advanced Settings menu, use the **▲** or **▼** keys to highlight the Records menu option. Touch **OK** to enter the menu shown in **Fig 4.01-1**.
- The **▲** or **▼** keys can be used to scroll through the records.
- To view a list of verification records for a particular user, enter the user's ID#.
- To return to a list of all the verifications records in a day, touch **ESC**.
- To view more details about a particular record, touch **OK** to view full screen.
- To return to a list of all the verifications records in a day, touch **ESC**.
- Touch **ESC** as necessary to exit all the menus.

NOTE: Only one day's verifications records can be displayed at a time. Upon entry into the menu, the device defaults to displaying the current day's verification records.

NOTE: Each record displayed in the menu consists of an ID# and a time that the verification was logged. If a verification failure is logged, a "?" is displayed in place of an ID#.

4.02 VERIFICATION FAILURES

- As an enrolled S-Admin, access the Advanced Settings menu by touching **MENU** on the keypad and verifying with the device.
- From the Advanced Settings menu, use the **▲** or **▼** keys to highlight the Records menu option. Touch **OK** to enter the menu.
- To view a list of all failed verifications for the date displayed in the upper right-hand corner of the menu, touch **MENU** to pop up menu selections. Use the **▲** or **▼** keys to highlight the "Denied Recs" option and then touch **OK**. (**Fig 4.02-1**)
- Only verification failures denoted by a "?" for the date displayed in the upper right-hand corner of the menu are displayed.
- To return to a list of all the verifications records for the date displayed in the upper right-hand corner of the menu, touch **ESC**.
- Touch **ESC** as necessary to exit all the menus.

4.03 RECORD VIEWING DATE

- a) As an enrolled S-Admin, access the Advanced Settings menu by touching **MENU** on the keypad and verifying with the device.
- b) From the Advanced Settings menu, use the **▲** or **▼** keys to highlight the Records menu option. Touch **OK** to enter the menu.
- c) To select a particular date to view verification records, touch **MENU** to pop up menu selections. Use the **▲** or **▼** keys to highlight the Specify Day option and then touch **OK**.
- d) Use the **▲** key to scroll from right to left and the **▼** key to scroll from left to right through the fields in the date screen. From left to right, set the year, the month and the day that records are to be viewed and then touch **OK**.
(Fig 4.03-1)
- e) Only verification records for the date displayed in the upper right-hand corner of the menu are displayed.
- f) Touch **ESC** as necessary to exit all the menus.

4.04 VIEWING THE PREVIOUS DAY'S RECORDS

- a) As an enrolled S-Admin, access the Advanced Settings menu by touching **MENU** on the keypad and verifying with the device.
- b) From the Advanced Settings menu, use the **▲** or **▼** keys to highlight the Records menu option. Touch **OK** to enter the menu.
- c) To set the viewing date back one day from the date displayed in the upper right-hand corner of the menu, touch **MENU** to pop up menu selections. Use the **▲** or **▼** keys to highlight the Prev Day option and then touch **OK**.
- d) The verification records for the new day will be displayed.
- e) Touch **ESC** as necessary to exit all the menus.

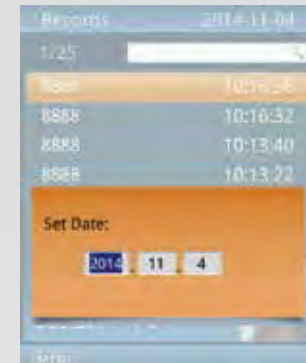


Fig 4.03-1

4.05 VIEWING THE NEXT DAY'S RECORDS

- a) As an enrolled S-Admin, access the Advanced Settings menu by touching **MENU** on the keypad and verifying with the device.
 - b) From the Advanced Settings menu, use the **▲** or **▼** keys to highlight the Records menu option. Touch **OK** to enter the menu.
 - c) To set the viewing date forward one day from the date displayed in the upper right-hand corner of the menu, touch **MENU** to pop up menu selections. Use the **▲** or **▼** keys to highlight the Next Day option and then touch **OK**.
- Note:** If it is today's date, the NEXT DAY option will not be highlighted.
- d) The verification records for the new day will be displayed.
 - e) Touch **ESC** as necessary to exit all the menus.

4.06 VIEWING A RECORD'S DETAILS

- a) As an enrolled S-Admin, access the Advanced Settings menu by touching **MENU** on the keypad and verifying with the device.
- b) From the Advanced Settings menu, use the **▲** or **▼** keys to highlight the Records menu option. Touch **OK** to enter the menu.
- c) The **▲** or **▼** keys can be used to scroll through the records.

NOTE: Each record displayed in the menu consists of an ID# and a time that the verification was logged. If a verification failure is logged, a "?" is displayed in place of an ID#.

- d) To view a list of verification records for a particular user, enter the user's ID#.
- e) Touch **OK** to view the Verification Record. *(Fig 4.06-1)*

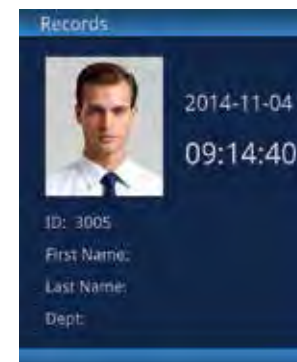


Fig 4.06-1

- f) The Verification Record can also be view by pressing **MENU** to pop up menu selections, using the **▲** or **▼** keys to highlight the Details option and then touching **OK**.
- g) To return to a list of all the verifications records for a selected viewing date, touch **ESC**.
- h) Touch **ESC** as necessary to exit all the menus.

Section 5: Access Control



5.01 Access Control Overview

5.02 Device Permissions

5.03 Door Settings

5.04 Door Lock Settings

5.05 Door Timer Setting

5.06 Guest PIN Access

5.07 Card # Parsing

5.08 Door Sensor Settings

5.09 Auxiliary Outputs & Inputs Overview

5.10 Auxiliary Outputs

5.11 Auxiliary Inputs

5.12 Wiegand Configuration

5.13 Silent Alarm

Section 5: Access Control

5.01 ACCESS CONTROL OVERVIEW

This menu provides control of 6 features: Device Permission, Door Settings, Door Sensor Settings, Auxiliary, Wiegand Config and Silent Alarm.

- As an enrolled S-Admin, access the Advanced Settings menu by touching **MENU** on the keypad and verifying with the device.
- From the Advanced Settings menu, use the **▲** or **▼** keys to highlight the Access Control menu option. Touch **OK** to enter the menu shown in *Fig 5.01-1*.
- Touch **ESC** as necessary to exit all the menus.

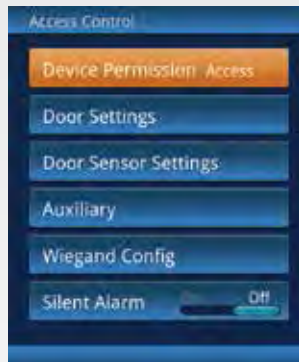


Fig 5.01- 1

5.02 DEVICE PERMISSIONS

When the device permission is set to “Access” permission is granted to the user once he/she has been verified. When the device permission is set to “Denied” permission is NOT granted to the user even though he/she has successfully verified. The permission is set to “Access” by default from the factory. Access permission for each user profile can be changed using a fully integrated access control system or the Stone Lock® Network (SLN) software application.

NOTE: Reference the applicable access control system user guide or reference sections of the Stone Lock® Network (SLN) User Guide.

A fully integrated access control system or the Stone Lock® Network (SLN) software application has the capability to set permissions per individual users. When the permission is set for an individual user, the device will comply with that user’s permission regardless of what this menu option has been set to (i.e. the user’s permission takes precedence). If a specific permission has not been set for a user, the setting of this menu option is used.

- As an enrolled S-Admin, access the Advanced Settings menu by touching **MENU** on the keypad and verifying with the device.
- From the Advanced Settings menu, use the **▲** or **▼** keys to highlight the Access Control menu option. Touch **OK** to enter the menu.
- From the Access Control menu, use the **▲** or **▼** keys to highlight the Device Permission menu option. Touch **OK** to enter the Device Permission: menu shown in *Fig 5.02-1*.
- Use the **▲** or **▼** keys to highlight the desired permission, “Access” or “Denied”.
- Touch **OK** to accept the selected permission or touch **ESC** to discontinue the process and return to the Access Control menu.
- When the permission has been changed, the “Setting Successful” screen will momentarily appear.
- Touch **ESC** as necessary to exit all the menus

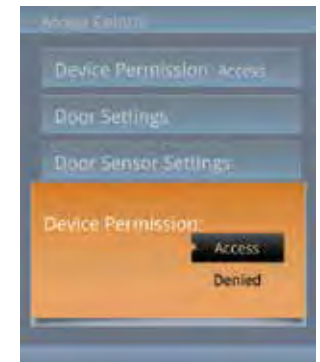


Fig 5.02-1

5.03 DOOR SETTINGS

This menu provides control of 6 features: Lock #1, Lock #2, Door Timer, Guest PIN, Guest PIN # and Card # Parsing. Lock #1 and Lock #2 are set to “Passive” from the factory.

- a) As an enrolled S-Admin, access the Advanced Settings menu by touching **MENU** on the keypad and verifying with the device.
- b) From the Advanced Settings menu, use the **▲** or **▼** keys to highlight the Access Control menu option. Touch **OK** to enter the menu.

- c) From the Access Control menu, use the **▲** or **▼** keys to highlight the Door Settings menu option. Touch **OK** to enter the Door Settings menu shown in **Fig 5.03-1**.

- d) Touch **ESC** as necessary to exit all the menus.

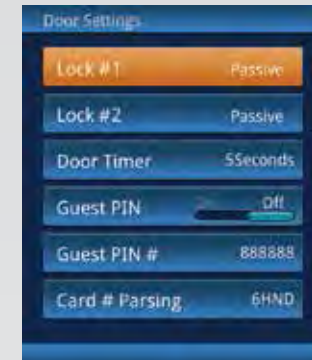


Fig 5.03-1

Lock Settings	Description
Passive	No voltage is supplied to the “Close”, “Open” or “EPOW” pins. The “Close” pins become the Normally Closed pins, the “Open” pins become the Normally Open pins and the “EPOW” pins become the Common pins of a standard relay. The “EPOW” pins are connected to the “Close” pins until after successful user verification when they are disconnected from the “Close” pins and connected to the “Open” pins. After the “Door Timer” time interval, the EPOW pins are disconnected from the “Open” pins and reconnected to the “Close” pins. See section 5.05 “Door Timer Setting”.
Active	Supplies 12 VDC, at the “Close” pins until after successful user verification. Then, no voltage is supplied until after the “Door Timer” time interval and then returns to 12 VDC. Supplies no voltage, at the “Open” pins until after successful user verification. Then, supplies 12 VDC until after the “Door Timer” time interval and then returns to a no voltage state. Supplies a continuous 12VDC at the “EPOW” pins. See section 5.05 “Door Timer Setting”.
Electric	Supplies a 5 VDC, 500ms pulse signal at the “Close” pins after successful user verification. Supplies a 5 VDC, 500ms pulse signal at the “Open” pins after the “Door Timer” time interval. Supplies a 5 VDC, 500ms pulse signal after successful user verification followed by another 5 VDC, 500ms pulse signal after the “Door Timer” time interval at the “EPOW” pins. See section 5.05 “Door Timer Setting”.



Fig 5.04-1

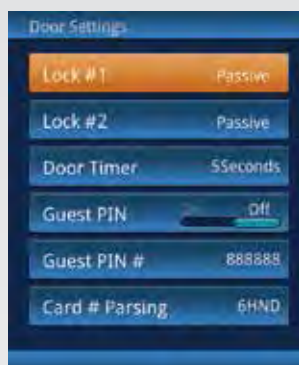


Fig 5.05-1



Fig 5.05-2

5.04 DOOR LOCK SETTINGS

Two lock controllers are available for use on the Stone Lock® Pro device and each can be controlled independently by using the Lock #1 and Lock #2 menu options in the Door Settings menu.

- As an enrolled S-Admin, access the Advanced Settings menu by touching **MENU** on the keypad and verifying with the device.
- From the Advanced Settings menu, use the **▲** or **▼** keys to highlight the Access Control menu option. Touch **OK** to enter the menu.
- From the Access Control menu, use the **▲** or **▼** keys to highlight the Door Settings menu option. Touch **OK** to enter the Door Settings menu. (*Fig 5.03-1, pg 31*)
- From the Door Settings menu, use the **▲** or **▼** keys to highlight the Lock #1 or the Lock #2 menu option. Touch **OK** to pop up the interface.
- Use the **▲** or **▼** keys to highlight the desired lock setting, “Passive” “Active” or “Electric” (*Fig 5.04-1*). Touch **OK**. The “Setting Successful” screen will momentarily appear.
- Touch **ESC** as necessary to exit all the menus.

5.05 DOOR TIMER SETTING

The Door Timer is the time interval between when a user has been verified and allowed access and when access is again denied until the next successful verification. For example, if the device is used to control a door lock, the lock will unlatch after verification of the user and latch again at the end of the set time interval.

- As an enrolled S-Admin, access the Advanced Settings menu by touching **MENU** on the keypad and verifying with the device.
- From the Advanced Settings menu, use the **▲** or **▼** keys to highlight the Access Control menu option. Touch **OK** to enter the menu.
- From the Access Control menu, use the **▲** or **▼** keys to highlight the Door Settings menu option. Touch **OK** to enter the Door Settings menu shown in *Fig 5.05-1*.
- From the Door Settings menu, use the **▲** or **▼** keys to highlight the Door Timer menu option. Touch **OK** to pop up the interface shown in *Fig 5.05-2*.
- Enter a Hold Open time interval that is between 0 and 120 seconds and touch **OK**. The “Setting Successful” screen will momentarily appear.

Note: When this parameter is set to 0, the actual hold open time interval is 0.5s.

- Touch **ESC** as necessary to exit all the menus.

5.06 GUEST PIN ACCESS

Guest PIN access provides the ability for a user to be granted access to the facility by entering a Guest PIN rather than by biometric verification. The use of this function is intended for temporary use only and will generate an alarm record.

To use the Guest PIN once it has been set up and turned on, touch **MENU**, enter the Guest PIN and touch OK. Use of the Guest PIN will be captured in the verification records with a photo of the individual along with a time and date stamp.

- a) As an enrolled S-Admin, access the Advanced Settings menu by touching **MENU** on the keypad and verifying with the device.
- b) From the Advanced Settings menu, use the ▲ or ▼ keys to highlight the Access Control menu option. Touch **OK** to enter the menu.
- c) From the Access Control menu, use the ▲ or ▼ keys to highlight the Door Settings menu option. Touch **OK** to enter the Door Settings menu.
- d) From the Door Settings menu, use the ▲ or ▼ keys to highlight the Guest PIN menu option. Touch **OK** to toggle the graphical switch from “Off” to “On” or from “On” to “Off”. The “On” setting allows the Guest PIN to be used to gain access. The “Off” setting does not allow the Guest PIN to be used to gain access.
- e) From the Door Settings menu, use the ▲ or ▼ keys to highlight the Guest Pin # menu option. Touch **OK** to pop up the interface shown in **Fig 5.06-1**.
- f) Enter a Guest PIN that is 4 to 8 digits in length and touch **OK**. The “Setting Successful” screen will momentarily appear.
- g) Touch **ESC** as necessary to exit all the menus.

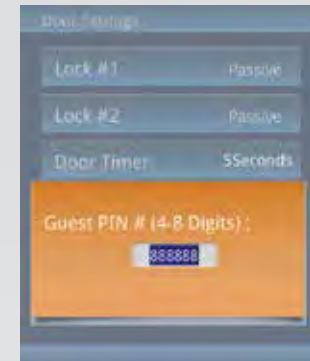


Fig 5.06-1

5.07 CARD # PARSING

This menu option provides the ability to change the method used by the Stone Lock® Pro device to interpret the information read from a card whose format has not been specifically pre-programmed into the device. Examples of preprogrammed formats include, 35 Bit Corporate 1000, 37 Bit H10304, 37 Bit H10302, and 37 Bit Andover Infinity.

Five different parsing modes are provided:

6HND*

6H8D

8H10D

2H4H

4H4H

***Note:** The default setting is 6HND.

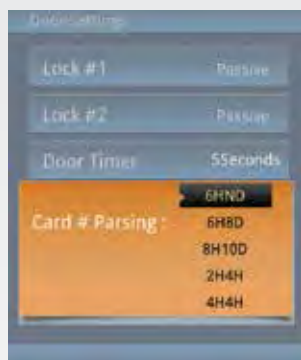


Fig 5.07-1

- As an enrolled S-Admin, access the Advanced Settings menu by touching **MENU** on the keypad and verifying with the device.
- From the Advanced Settings menu, use the **▲** or **▼** keys to highlight the Access Control menu option. Touch **OK** to enter the menu.
- From the Access Control menu, use the **▲** or **▼** keys to highlight the Door Settings menu option. Touch **OK** to enter the Door Settings menu.
- From the Door Settings menu, use the **▲** or **▼** keys to highlight the Card # Parsing menu option. Touch **OK** to enter the Card # Parsing menu shown in **Fig 5.07-1**.
- Use the **▲** or **▼** keys to highlight the desired setting. Touch **OK**. The "Setting Successful" screen will momentarily appear.
- Touch **ESC** as necessary to exit all the menus.

Designator	Format
6HND Default	Convert the last 6 Hexadecimal digits (i.e. 24 bits of a 26 bit card after excluding the parity bits) into a Decimal card number without limiting the amount of Decimal digits displayed. For example: "0110 1111 0110 1100 0011 1010" card bits = "6F6C3A" in Hexadecimal and is converted to "7302202" Decimal.
6H8D	Convert the last 6 Hexadecimal digits (i.e. 24 bits of a 26 bit card after excluding the parity bits) into an 8 digit Decimal card number. For example: "0110 1111 0110 1100 0011 1010" card bits = "6F6C3A" in Hexadecimal and is converted to "07302202" Decimal.
8H10D	Convert the last 8 Hexadecimal digits (i.e. 32 bits of a 34 bit card after excluding the parity bits) into an 10 digit Decimal card number. For example: 0000 0010 0110 1111 0110 1100 0011 1010" card bits = "026F6C3A" in Hexadecimal and is converted to "0040856634" Decimal.
2H4H	Of the last 6 Hexadecimal digits (i.e. 24 bits of a 26 bit card after excluding the parity bits), convert the first 2 Hexadecimal digits into a 3 digit Decimal number, then convert the latter 4 Hexadecimal digits into a 5 digit Decimal number. For example: "0110 1111 0110 1100 0011 1010" card bits = "6F6C3A" in Hexadecimal. "6F" is converted to "111" and "6C3A" is converted to "27706" and displayed as "11127706".
4H4H	Of the last 8 Hexadecimal digits (i.e. 32 bits of a 34 bit card after excluding the parity bits), convert the first 4 Hexadecimal digits into a 5 digit Decimal number then convert the latter 4 Hexadecimal digits into a 5 digit Decimal number. For example: "0000 0010 0110 1111 0110 1100 0011 1010" card bits = "026F6C3A" in Hexadecimal. "026F" is converted to "00623" and "6C3A" is converted to "27706" and displayed as "0062327706".

WARNING

During enrollment, if cards that have formats that have not been preprogrammed into the device are assigned to users read under one mode, these cards will no longer be interpreted by the device as valid once the device has been set to a different mode.

5.08 DOOR SENSOR SETTINGS

Using the “Door Sensor Inputs” on the device, the “Door Sensor Settings” are used to detect a forced entry or a held open condition.

For a forced entry condition, an alarm record is generated immediately when a Door Sensor Input detects a transition from a low state of 0.0 VDC to its default high state of 4.0 VDC without a prior successful user verification.

For a held open condition, an alarm record is generated when a successful verification has occurred and the Door Sensor Input detects a transition from a low state of 0.0 VDC to its default high state of 4.0 VDC but does not detect a transition back to a low state prior to the “Door Timeout” period expiring.

The “Door Timeout” period starts when the low to high transition is detected at the Door Sensor Input. “Door Sensor Input 1” is used for the primary door and “Door Sensor Input 2” is used for the secondary door.

- a) As an enrolled S-Admin, access the Advanced Settings menu by touching **MENU** on the keypad and verifying with the device.
- b) From the Advanced Settings menu, use the **▲** or **▼** keys to highlight the Access Control menu option. Touch **OK** to enter the menu.
- c) From the Access Control menu, use the **▲** or **▼** keys to highlight the Door Sensor Settings menu option. Touch **OK** to enter the Door Sensor Settings menu shown in **Fig 5.08-1**.
- d) From the Door Sensor Settings menu, use the **▲** or **▼** keys to highlight the “Detect” menu option. Touch **OK** to toggle the graphical switch from “Off” to “On” or from “On” to “Off”. The “On” setting detects a forced entry or a held open condition and generates an alarm record. The “Off” setting does not detect a forced entry or a held open condition.
- e) From the Door Sensor Settings menu, use the **▲** or **▼** keys to highlight the Door Timeout menu option. Touch **OK** to pop up the interface shown in **Fig 5.08-2**.
- f) Enter a Door Sensor Timeout interval that is between 3 and 120 seconds and touch **OK**. The “Setting Successful” screen will momentarily appear.
- g) Touch **ESC** as necessary to exit all the menus.

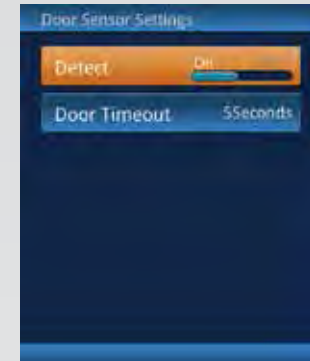


Fig 5.08-1



Fig 5.08-2

5.09 AUXILIARY OUTPUTS AND INPUTS

The Auxiliary menu provides the ability to control the function of all Stone Lock® Pro Auxiliary Outputs and Inputs.

- As an enrolled S-Admin, access the Advanced Settings menu by touching **MENU** on the keypad and verifying with the device.
- From the Advanced Settings menu, use the ▲ or ▼ keys to highlight the Access Control menu option. Touch **OK** to enter the menu.
- From the Access Control menu, use the ▲ or ▼ keys to highlight the Auxiliary menu option. Touch **OK** to enter the Auxiliary menu shown in **Fig 5.09-1**.
- Touch **ESC** as necessary to exit all the menus.

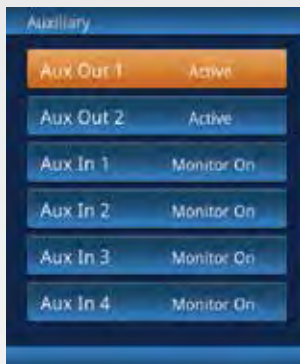


Fig 5.09-1

5.10 AUXILIARY OUTPUTS

Two auxiliary outputs are available for use on the Stone Lock® Pro device and each can be controlled independently by using the “Aux Out 1” and “Aux Out 2” menu options in the Auxiliary menu. The outputs can be configured to change state based on designated alarm events.

Reference Section 7.04, Alarm Settings.

- As an enrolled S-Admin, access the Advanced Settings menu by touching **MENU** on the keypad and verifying with the device.
- From the Advanced Settings menu, use the ▲ or ▼ keys to highlight the Access Control menu option. Touch **OK** to enter the menu.
- From the Access Control menu, use the ▲ or ▼ keys to highlight the Auxiliary menu option. Touch **OK** to enter the Auxiliary menu shown above in **Fig 5.09-1**.

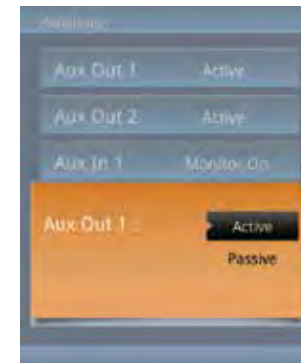


Fig 5.10-1

- From the Auxiliary menu, use the ▲ or ▼ keys to highlight the “Aux Out 1” or the “Aux Out 2” menu option. Touch **OK** to pop up the interface shown in **Fig 5.10-1**.
- Use the ▲ or ▼ keys to highlight the desired Output Type, “Passive” or “Active”. Touch **OK**. The “Setting Successful” screen will momentarily appear.
- Touch **ESC** as necessary to exit all the menus.

Output Type	Description
Passive	No voltage is supplied to the “Normally Closed (NC)”, “Normally Opened (NO)” or “Common (COM)” pins. The “NC” pins become the Normally Closed pins, the “NO” pins become the Normally Open pins and the “COM” pins become the Common pins of a standard relay. The “COM” pins are connected to the “NC” pins until after a designated alarm event occurs when they are disconnected from the “NC” pins and connected to the “NO” pins. After approximately 6 seconds, the “COM” pins are disconnect from the “NO” pins and reconnected to the “NC” pins.
Active Default Setting	Supplies 12 VDC, at the “Normally Closed (NC)” pins until after a designated alarm event occurs. Then, supplies no voltage for approximately 6 seconds and then returns to 12 VDC. Supplies no voltage at the “Normally Opened (NO)” pins until after a designated alarm event occurs. Then, supplies 12 VDC for approximately 6 seconds and then returns to a no voltage state. Supplies a continuous 12VDC at the “Common (COM)” pins. This is the default setting.

5.11 AUXILIARY INPUTS

Four auxiliary Inputs are available for use on the Stone Lock® Pro device and each can be controlled independently by using the “Aux In 1”, “Aux In 2”, “Aux In 3” and “Aux In 4” menu options in the Auxiliary menu.

- As an enrolled S-Admin, access the Advanced Settings menu by touching **MENU** on the keypad and verifying with the device.
- From the Advanced Settings menu, use the **▲** or **▼** keys to highlight the Access Control menu option. Touch **OK** to enter the menu.
- From the Access Control menu, use the **▲** or **▼** keys to highlight the Auxiliary menu option. Touch **OK** to enter the Auxiliary menu shown in **Fig 5.09-1**.
- From the Auxiliary menu, use the **▲** or **▼** keys to highlight the “Aux In 1”, “Aux In 2”, “Aux In 3” or “Aux In 4” menu option. Touch **OK** to pop up the interface shown in **Fig 5.11-1**.
- Use the **▲** or **▼** keys to highlight the desired Input Type, “NO” or “NC”. Touch **OK**. The “Setting Successful” screen will momentarily appear.
- Touch **ESC** as necessary to exit all the menus.

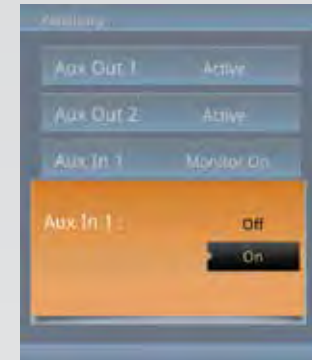


Fig 5.11-1

Input Type	Description
NO	When this menu option is chosen, an event is detected when the Auxiliary input detects a transition from a low state of 0.0 VDC to its default high state of 4.0 VDC. This can be accomplished by disconnecting the Auxiliary Input from ground or driving it high with a TTL signal.
NC	When this menu option is chosen, an event is detected when the Auxiliary input detects a transition from its default high state of 4.0 VDC to a low state of 0.0 VDC. This can be accomplished by connecting the Auxiliary Input to ground or driving it low with a TTL signal.



Fig 5.12-1



Fig 5.12-2

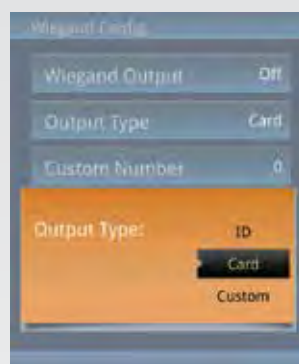


Fig 5.12-3



Fig 5.12-4

5.12 WIEGAND CONFIGURATION

This “Wiegand Config” menu option provides the ability to activate and de-activate the Wiegand output on the control unit and to set the type information that is communicated at the Wiegand output. Three types of information can be communicated:

1. ID Number
2. Card Number
3. Customer Number

ID Number:

If the output type is set to “ID”, then upon successful verification of a user, independent of the Recognition Mode used (1:N, 1:1 or Card Only), the user’s ID number will be communicated at the Wiegand output as a 26 bit or 34 bit Wiegand (depending on the Wiegand Output setting) with no Facility Code.

The largest ID number that can be sent under this scenario when the Wiegand Output setting is 26 is 16777215. All ID numbers larger than 16777215 will be truncated (ex. 16777216, will be sent as 0, 16777217 will be sent as 1 and so on). The largest ID number that can be sent when the Wiegand Output Setting is 34 is 4294967295. All ID numbers larger than 4294967295 will be sent as 4294967295.

Card Number:

If the output type is set to “Card” and the Recognition Mode is set to “1:N”, then upon successful verification of a user, the card number stored in the user’s profile will be communicated at the Wiegand output as a 26 bit or 34 bit Wiegand (depending on the Wiegand Output setting) with no Facility Code.

The largest Card number that can be sent under this scenario when the Wiegand Output setting is 26 is 16777215. All card numbers larger than 16777215 will be truncated (ex. 16777216, will be sent as 0, 16777217 will be sent as 1 and so on). The largest Card number that can be sent when the Wiegand Output Setting is 34 is 4294967295. All Card numbers larger than 4294967295 will be sent as 4294967295.

If the Output Type is set to “Card” and the Recognition Mode is set to “1:1”, then upon successful verification of a user, the Wiegand Output setting is ignored and all the bits read from the user’s card during verification are communicated at the Wiegand output.

Custom Number:

If the output type is set to “Custom” then upon successful verification of any user, independent

of the Recognition Mode used (1:N, 1:1 or Card Only), a custom number will be communicated at the Wiegand output as a 26 Bit or 34 Bit Wiegand (depending on the Wiegand Output setting) with no Facility Code.

The largest Custom number that can be sent under this scenario when the Wiegand Output setting is 26 is 16777215. All Custom numbers larger than 16777215 will be truncated (ex. 16777216, will be sent as 0, 16777217 will be sent as 1 and so on). The largest Custom number that can be sent when the Wiegand Output Setting is 34 is 99999999.

***Note:** The Custom Number is specific to a device not a user. Therefore, every successful verification of a user at one device will communicate the same Custom number at the Wiegand output.

- a) As an enrolled S-Admin, access the Advanced Settings menu by touching **MENU** on the keypad and verifying with the device.
- b) From the Advanced Settings menu, use the **▲** or **▼** keys to highlight the Access Control menu option. Touch **OK** to enter the menu.
- c) From the Access Control menu, use the **▲** or **▼** keys to highlight the Wiegand Config menu option. Touch **OK** to enter the Wiegand Config menu shown in **Fig 5.12-1**.

- d) From the Wiegand Config menu, use the **▲** or **▼** keys to highlight the Wiegand Output menu option. Touch **OK** to pop up the interface shown in **Fig 5.12-2**.
- e) Use the **▲** or **▼** keys to highlight the desired format type, "OFF", "26" or "34". Touch **OK**. The "Setting Successful" screen will momentarily appear.
- f) From the Wiegand Config menu, use the **▲** or **▼** keys to highlight the Output Type menu option. Touch **OK** to pop up the interface shown in **Fig 5.12-3**.
- g) Use the **▲** or **▼** keys to highlight the desired Output Type, "ID", "Card" or "Custom". Touch **OK**. The "Setting Successful" screen will momentarily appear.
- h) If the output type is set to "Custom", from the Wiegand Config menu, use the **▲** or **▼** keys to highlight the Custom number menu option. Touch **OK** to pop up the interface shown in **Fig 5.12-4**.
- i) Enter a custom number that is 1 to 8 digits in length and touch **OK**. The "Setting Successful" screen will momentarily appear.
- j) Touch **ESC** as necessary to exit all the menus.

Output Type	Description
ID	Upon successful verification of a user, the user's ID number will be communicated at the Wiegand output
Card	Upon successful verification of a user, the card number stored in the user's profile (if the Recognition Mode is set to "1:N") or the card information read from a presented card (if the Recognition Mode is set to "1:1") is communicated at the Wiegand output.
Custom	Upon successful authentication of a user, a custom number # will be communicated at the Wiegand output.

Wiegand Output	Description
Off	The Wiegand output is turned off.
26	The Wiegand output is turned on and set to 26 bits per packet to communicate ID numbers or Card numbers stored in a user's profile as well as Custom numbers. This setting is ignored for cards presented during verification when all of the bits read from the card will be communicated at the Wiegand output.
34	The Wiegand output is turned on and set to 34 bits per packet to communicate ID numbers or Card numbers stored in a user's profile as well as Custom numbers. This setting is ignored for cards presented during verification when all of the bits read from the card will be communicated at the Wiegand output.

Notes:**5.13 Silent Alarm**

This function provides the capability for users to trip a silent alarm in case of emergencies. When the function is turned on, all users are required to first touch either the **OK** button (or any number key on the keypad) prior to biometric verification (or present card or enter PIN when in 1:1 mode) to gain normal access. To trip the silent alarm, the user must first touch and hold ESC for approximately 5 seconds until the “Verifying” screen appears and then present their face for verification. Once the verification is successful, the silent alarm will be sent over the LAN connection.

- a) As an enrolled S-Admin, access the Advanced Settings menu by touching **MENU** on the keypad and verifying with the device.
- b) From the Advanced Settings menu, use the **▲** or **▼** keys to highlight the Access Control menu option. Touch **OK** to enter the menu.
- c) From the Access Control menu, use the **▲** or **▼** keys to highlight the Silent Alarm menu option. Touch **OK** to toggle the graphical switch from “Off” to “On” or from “On” to “Off”.
- d) Touch **ESC** as necessary to exit all the menus.

Section 6: Network Functions



6.01 Network Functions

6.02 LAN

6.03 IP Settings

6.04 Setting Up the IP Address

6.05 Setting the Subnet Mask

6.06 Setting the Gateway Address

6.07 Setting the DNS Address

6.08 Web Service

6.09 Real-Time Records

6.10 Remote

6.11 Auto Upload New User

Section 6: Network Functions

6.01 NETWORK FUNCTIONS

The “Network” menu provides six menu options:

- LAN
- IP Settings
- Web Service
- Real-Time Records
- Remote Load
- Auto Upload New User.

LAN, IP Settings and Web Service can be modified locally at the device. The other three can have their status viewed at the device but can only be modified using a fully integrated access control system or the Stone Lock® Network (SLN) software application.

- As an enrolled S-Admin, access the Advanced Settings menu by touching **MENU** on the keypad and verifying with the device.
- From the Advanced Settings menu, use the **▲** or **▼** keys to highlight the Network menu option. Touch **OK** to enter the Network menu shown in **Fig 6.01-1**
- Touch **ESC** as necessary to exit all the menus.

6.02 LAN

The “LAN” menu option provides the ability to activate and de-activate the Ethernet network connection. When a fully integrated access control system or the Stone Lock® Network (SLN) software application is used with the device, the “On” option will need to be selected for the device to communicate. If a fully integrated access control system or the SLN is not being used, it is recommended that the “Off” option be selected.

- As an enrolled S-Admin, access the Advanced Settings menu by touching **MENU** on the keypad and verifying with the device.
- From the Advanced Settings menu, use the **▲** or **▼** keys to highlight the Network menu option. Touch **OK** to enter the Network menu.



Fig 6.01-1

- From the Network menu, use the **▲** or **▼** keys to highlight the LAN menu option. Touch **OK** to enter the LAN: menu shown in **Fig 6.02-1**.
- Use the **▲** or **▼** keys to highlight “On” to enable the Ethernet network connection or “Off” to disable the Ethernet network connection.
- Touch **OK** to accept the highlighted selection. The “Setting Successful” screen will momentarily appear. Touch **ESC** to discontinue the process and return to the Network menu.
- Touch **ESC** as necessary to exit all the menus.



Fig 6.02-1

6.03 IP SETTINGS

The IP Settings menu provides five menu options:

- IP Address
- Subnet Mask
- Gateway
- DNS
- Multicast

The first four can be modified at the device. The last one can only have its status viewed at the device.

- As an enrolled S-Admin, access the Advanced Settings menu by touching **MENU** on the keypad and verifying with the device.
- From the Advanced Settings menu, use the **▲** or **▼** keys to highlight the Network menu option. Touch **OK** to enter the Network menu.
- From the Network menu, use the **▲** or **▼** keys to highlight the IP Settings menu option. Touch **OK** to enter the IP Settings menu.
- Touch **ESC** as necessary to exit all the menus.

6.04 SETTING THE IP ADDRESS

- As an enrolled S-Admin, access the Advanced Settings menu by touching **MENU** on the keypad and verifying with the device.
- From the Advanced Settings menu, use the **▲** or **▼** keys to highlight the Network menu option. Touch **OK** to enter the Network menu.
- From the Network menu, use the **▲** or **▼** keys to highlight the IP Settings menu option. Touch **OK** to enter the IP Settings menu shown in **Fig 6.04-1**.
- To set the IP Address, use the **▲** or **▼** keys to highlight the IP Address option and then touch **OK** to view the “Set IP Address” screen shown in **Fig 6.04-2**.
- Use the **▲** key to scroll from right to left and the **▼** key to scroll from left to right through the fields in the “Set IP Address:” screen. Enter the desired IP Address and touch **OK** or touch **ESC** to leave the address unchanged and return to the IP Settings menu.
- Touch **ESC** as necessary to exit all the menus.



Fig 6.04-1



Fig 6.04-2



Fig 6.05-1

6.05 SETTING THE SUBNET MASK

- a) As an enrolled S-Admin, access the Advanced Settings menu by touching **MENU** on the keypad and verifying with the device.
- b) From the Advanced Settings menu, use the **▲** or **▼** keys to highlight the Network menu option. Touch **OK** to enter the Network menu.
- c) From the Network menu, use the **▲** or **▼** keys to highlight the IP Settings menu option. Touch **OK** to enter the IP Settings menu shown in **Fig 6.04-1**.
- d) To set the Subnet Mask, use the **▲** or **▼** keys to highlight the “Subnet Mask” option and then touch **OK** to view the “Set subnet Mask:” screen shown in figure **Fig 6.05-1**.
- e) Use the **▲** key to scroll from right to left and the **▼** key to scroll from left to right through the fields in the “Set subnet Mask:” screen. Enter the desired Subnet Mask and touch **OK** or touch **ESC** to leave the Subnet Mask unchanged and return to the “IP Settings” menu.
- f) Touch **ESC** as necessary to exit all the menus.

6.06 SETTING THE GATEWAY ADDRESS

- a) As an enrolled S-Admin, access the Advanced Settings menu by touching **MENU** on the keypad and verifying with the device.
- b) From the Advanced Settings menu, use the **▲** or **▼** keys to highlight the Network menu option. Touch **OK** to enter the Network menu.
- c) From the Network menu, use the **▲** or **▼** keys to highlight the IP Settings menu option. Touch **OK** to enter the IP Settings menu shown in **Fig 6.06-1**.
- d) To set the Gateway Address, use the **▲** or **▼** keys to highlight the “Gateway” option and then touch **OK** to view the “Set Gateway:” screen shown in figure **Fig 6.06-2**.
- e) Use the **▲** key to scroll from right to left and the **▼** key to scroll from left to right through the fields in the “Set Gateway:” screen. Enter the desired Gateway Address and touch **OK** or touch **ESC** to leave the Gateway Address unchanged and return to the IP Settings menu.
- f) Touch **ESC** as necessary to exit all the menus.

6.07 SETTING THE DNS ADDRESS

- a) As an enrolled S-Admin, access the Advanced Settings menu by touching **MENU** on the keypad and verifying with the device.
- b) From the Advanced Settings menu, use the **▲** or **▼** keys to highlight the Network menu option. Touch **OK** to enter the Network menu.
- c) From the Network menu, use the **▲** or **▼** keys to highlight the IP Settings menu option. Touch **OK** to enter the IP Settings menu shown above in **Fig 6.06-1**.
- d) To set the DNS Address, use the **▲** or **▼** keys to highlight the DNS option and then touch **OK** to view the “Set DNS:” screen.
- e) Use the **▲** key to scroll from right to left and the **▼** key to scroll from left to right through the fields in the “Set DNS:” screen. Enter the desired DNS Address and touch **OK** or touch **ESC** to leave the DNS Address unchanged and return to the IP Settings menu.
- f) Touch **ESC** as necessary to exit all the menus.



Fig 6.06-1

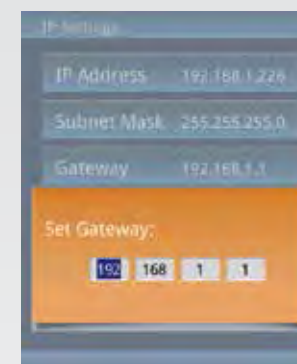


Fig 6.06-2

6.08 WEB SERVICE

This menu is used to turn on and off “Load Users”, “Write Users”, “Write Records” and “Sync Time” web service features.

Note: This option is only available in certain markets.

The “Load User” features provides the ability for the device to access user profiles in a database on a network server over the web using a web service application without it storing any of them locally. This feature is only available when the verification mode is 1:1 (biometric and a Card or ID # as a secondary verification).



Fig 6.08-1

The “Write Users” feature automatically synchronizes a new user’s profile (information and biometric signature data) to a database on a network server over the web using a web service application after enrollment has been completed at the device. If the profile contains an unused ID #, the profile will be directly stored in the database. If the profile contains a used ID #, the profile associated with that ID # in the database will be overwritten.

The “Write Records” feature provides the ability for the device to provide verification information and alarm events as they happen over the web using a web service application.

The “Sync Time” feature provides the ability for the device to synchronize its internal clock over the web using a web service application.

- a) As an enrolled S-Admin, access the Advanced Settings menu by touching **MENU** on the keypad and verifying with the device.
- b) From the Advanced Settings menu, use the **▲** or **▼** keys to highlight the Network menu option. Touch **OK** to enter the Network menu.
- c) From the Network menu, use the **▲** or **▼** keys to highlight the Web Service menu option. Touch **OK** to enter the Web Service settings menu shown in **Fig 6.08-1**.
- d) From the Web Service settings menu, use the **▲** or **▼** keys to highlight the Load Users menu option. Touch **OK** to toggle the graphical switch from “Off to “On” or from “On” to “Off”.
- e) From the Web Service settings menu, use the **▲** or **▼** keys to highlight the Write Users menu option. Touch **OK** to toggle the graphical switch from “Off” to “On” or from “On” to “Off”.
- f) From the Web Service settings menu, use the **▲** or **▼** keys to highlight the Write Records menu option. Touch **OK** to toggle the graphical switch from “Off to “On” or from “On” to “Off”.
- g) From the Web Service settings menu, use the **▲** or **▼** keys to highlight the Sync Time menu option. Touch **OK** to toggle the graphical switch from “Off to “On” or from “On” to “Off”.
- h) Touch **ESC** as necessary to exit all the menus.

Notes:**6.10 REMOTE LOAD**

The “Remote Load” feature provides the ability for the device to access user profiles in a database on a network server without it storing any of them locally.

This feature is only available when the verification mode is 1:1 (biometric and a Card or ID # as a secondary verification). The state (“On” or “Off”) of the “Remote Load” option can be viewed at the Stone Lock® Pro device. However, it can only be changed to “On” or “Off” through a fully integrated access control system or by checking or un-checking respectively the “Remote Load” option under the “Device Status” tab in the “Device Management” menu of the Stone Lock® Network (SLN) software application. **Reference Section 2.3.1 Device Management**, of the Stone Lock® Network User Guide.

When set to “On” and connected to the SLN, a device can verify any user found in the SLN database that has a card or ID # associated with that user’s biometric profile even if that profile does NOT reside on the device.

This feature provides the ability for devices, when connected to the SLN, to verify a quantity of users that is limited only by the disk storage space where the SLN database resides if (card and face) or (ID # and face) verification is used.

6.11 AUTO UPLOAD NEW USER

The “Auto Upload New User” feature automatically synchronizes a new user’s profile (information and biometric signature data) with a fully integrated access control system or the Stone Lock® Network (SLN) software application after enrollment has been completed at the device.

If the profile contains an unused ID #, the profile will be directly stored in the access control system’s or SLN’s database. If the profile contains a used ID #, the profile associated with that ID # in the access control system or in the SLN database will be overwritten. The state (“On” or “Off”) of the “Auto Upload New User” option can be viewed at the Stone Lock® Pro device. However, it can only be changed to “On” or “Off” through a fully integrated access control system or by checking or un-checking respectively the “Auto Upload New User” option under the “Device Status” tab in the “Device Management” menu of the SLN. **Reference Section 2.3.1 “Device Management”** of the Stone Lock® Network User Guide.

When set to “On” and connected to the SLN, enrolled users can be synchronized between the device and the SLN.

Section 7: System Settings



- | | | |
|-------------------------------|--|-----------------------------------|
| 7.01 System Settings | 7.10 Impact Sensitivity | 7.17 Setting User Interval |
| 7.02 Delete Users/Recs | 7.11 Setting Verification Modes | 7.18 Date/Time |
| 7.03 Security Level | 7.12 Setting Biometric Facial Recognition Only | 7.19 Time Settings |
| 7.04 Alarm Settings | 7.13 Setting Biometric Facial Recognition with a Secondary Verification | 7.20 Date Settings |
| 7.05 Arm/Disarm Alarms | 7.14 Setting Mixed Mode | 7.21 USB Operations |
| 7.06 SMS Module | 7.15 Setting Card Only | 7.22 Program Update |
| 7.07 Event Linkage | 7.16 Encrypting the User Information Upon Verification | 7.23 Records Download |
| 7.08 Aux In Linkage | | 7.24 User Download |
| 7.09 Wireless Linkage | | 7.25 User Upload |



Fig 7.01-1

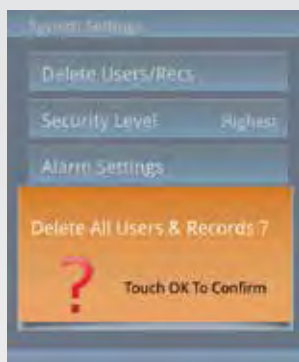


Fig 7.02-1

7.01 SYSTEM SETTINGS

In the System Settings menu, there are six menu options:

- Delete Users/Recs
- Security Level
- Alarm Settings
- Verification Mode
- Date/Time
- USB Operations (USB options accessible only when a USB drive is detected).

- a) As an enrolled S-Admin, access the Advanced Settings menu by touching **MENU** on the keypad and verifying with the device.
- b) From the Advanced Settings menu, use the **▲** or **▼** keys to highlight the System Settings menu option. Touch **OK** to enter the System Settings menu shown in **Fig 7.01-1**.
- c) Touch **ESC** as necessary to exit all the menus.

7.02 DELETE USERS/RECS

This menu option provides the capability to delete all user profiles, including the S-Admin / Admin profiles and all verification records stored in the Stone Lock® Pro device.

***Note:** All other menu option settings remain unchanged including the verification mode of 1:1, 1:N, Mixed and Card Only.

Warning
Once the above process has been performed, the user profiles and the verification records cannot be restored.

- a) As an enrolled S-Admin, access the Advanced Settings menu by touching **MENU** on the keypad and verifying with the device.
- b) From the Advanced Settings menu, use the **▲** or **▼** keys to highlight the System Settings menu option. Touch **OK** to enter the System Settings menu. (**Fig 7.01-1**)
- c) From the System Settings menu, use the **▲** or **▼** keys to highlight the Delete Users/Recs menu option. Touch **OK** to pop up the “Delete All Users & Records?” dialogue box (**Fig 7.02-1**)
- d) Touch **OK** to delete all user profiles and verification records or touch **ESC** to discontinue the process and return to the “System Settings” menu.
- e) Touch **ESC** as necessary to exit all the menus.

7.03 SECURITY LEVEL

This menu option provides the ability to increase or decrease the level of security. The setting that provides the greatest accuracy is the “Highest” setting. This is the factory default setting. If the device is set to “Higher” or “High”, it is highly recommended that the verification mode be set to 1:1. (**Reference Section 7.13**)

- a) As an enrolled S-Admin, access the Advanced Settings menu by touching **MENU** on the keypad and verifying with the device.
- b) From the Advanced Settings menu, use the **▲** or **▼** keys to highlight the System Settings menu option. Touch **OK** to enter the System Settings menu.
- c) From the System Settings menu, use the **▲** or **▼** keys to highlight the Security Level menu option. Touch **OK** to access the Security Level: menu. (**Fig 7.03-1**)
- d) Use the **▲** or **▼** keys to highlight the desired Security Level:
 - High
 - Higher
 - Highest
- e) Touch **OK** to accept the selected security level or touch **ESC** to discontinue the process and return to the System Settings menu.
- f) When the security level has been changed, the “Setting Successful” screen will momentarily appear.
- g) Touch **ESC** as necessary to exit all the menus.

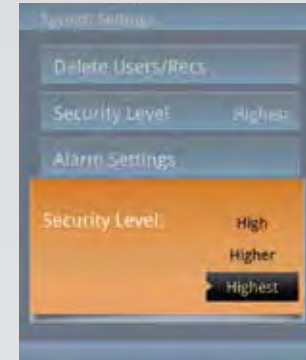


Fig 7.03-1

7.04 ALARM SETTINGS

This menu provides the capability to arm alarms that can be triggered by either detected events, a change in state detected at one of the four Auxiliary Inputs or events detected at wireless sensors.

There are six menu options:

- Arm / Disarm
- SMS Module
- Event Linkage
- Aux In Linkage
- Wireless Linkage
- Impact Sensitivity

Each alarm input can be set to generate an output signal at one or all of the following:

- Auxiliary Output 1
- Auxiliary Output 2
- SMS Module

For signals to be generated at the Auxiliary Outputs, the outputs must be turned on.

Reference Section 5.10 Auxiliary Outputs.



Fig 7.04-1

This menu also provides an option for setting the level of impact sensitivity.

- As an enrolled S-Admin, access the Advanced Settings menu by touching **MENU** on the keypad and verifying with the device.
- From the Advanced Settings menu, use the **▲** or **▼** keys to highlight the System Settings menu option. Touch **OK** to enter the System Settings menu.
- From the System Settings menu, use the **▲** or **▼** keys to highlight the Alarm Settings menu option. Touch **OK** to access the Alarm Settings menu. (**Fig 7.04-1**)
- Touch **ESC** as necessary to exit all the menus.

7.05 Arm / Disarm Alarms

When the Arm / Disarm menu option is set to “On”, each tripped alarm will generate a signal at its configured output(s). No signals are generated at the configured outputs when the menu option is set to “Off” except for the wireless smoke and gas sensors. **Reference Sections 7.07 (Event Linkage), 7.08 (Aux In Linkage) and 7.09 (Wireless Linkage).**

Regardless of the switch position, all alarms are sent to a fully integrated access control systems or to the Stone Lock® Network (SLN) software application. After one successful user verification, the “Arm / Disarm” menu option is automatically set to “off”.

- As an enrolled S-Admin, access the Advanced Settings menu by touching **MENU** on the keypad and verifying with the device.
- From the Advanced Settings menu, use the **▲** or **▼** keys to highlight the System Settings menu option. Touch **OK** to enter the System Settings menu.
- From the System Settings menu, use the **▲** or **▼** keys to highlight the Alarm Settings menu option. Touch **OK** to access the Alarm Settings menu.
- From the Alarm Settings menu, use the **▲** or **▼** keys to highlight the Arm / Disarm menu option. Touch **OK** to toggle the graphical switch from “Off to “On” or from “On” to “Off”. The “On” setting “Arms” the alarms. The “Off” setting “Disarms” the alarms.
- Touch **ESC** as necessary to exit all the menus.

7.06 SMS MODULE

Notification of a triggered alarm from an Event, Input or Wireless Linkage can be sent to a mobile device. When the Event Linkages of denied user, faceplate removed, or impact alarms are set, triggering of these alarms will be sent via MMS. All other alarms whose linkages have been set will be sent via SMS. The first mobile ID will receive alarms sent by SMS in 7 seconds and alarms sent by MMS in 25 seconds.

Note: This option is only available in certain markets.

- a) As an enrolled S-Admin, access the Advanced Settings menu by touching **MENU** on the keypad and verifying with the device.
- b) From the Advanced Settings menu, use the ▲ or ▼ keys to highlight the System Settings menu option. Touch **OK** to enter the System Settings menu.
- c) From the System Settings menu, use the ▲ or ▼ keys to highlight the Alarm Settings menu option. Touch **OK** to access the Alarm Settings menu.
- d) From the Alarm Settings menu, use the ▲ or ▼ keys to highlight the SMS Module menu option. Touch **OK** to access the SMS Module menu.
- e) Touch **OK** to toggle the graphical switch from “Off” to “On”.
- f) When the “SMS/MMS” graphical switch is in the “On” position, the ▲ or ▼ keys can be used to highlight any of the Mobile ID# menu options. Select one and touch **OK** to access the menu option. (Fig 7.06-1)
- g) In the Mobile ID# menu, enter any valid mobile number up to 13 digits long. Use the ◀ key to backspace if necessary. (Fig 7.06-2)
- h) Touch **OK** to accept the number or touch **ESC** to discontinue the process and return to the SMS Module menu.
- i) When the mobile number has been accepted, the “Setting Successful” screen will momentarily appear.
- j) Touch **ESC** as necessary to exit all the menus.

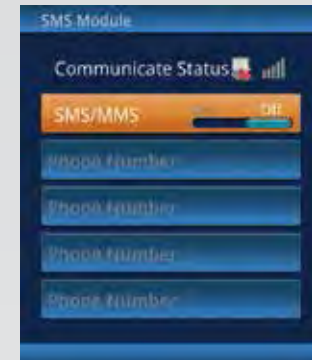


Fig 7.06-1

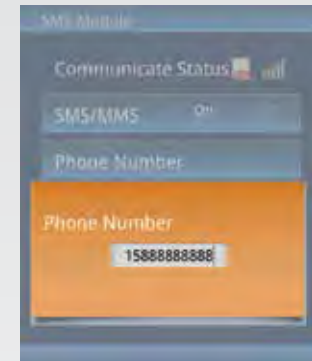


Fig 7.06-2

7.07 EVENT LINKAGE

This menu option provides the following events that can be detected:

- Denied User
- Battery Backup
- Open Door Alert
- Forced Entry
- Faceplate Removed
- Impact Alarm



Fig 7.07-1

These events can be set to generate an output signal at one or all of the following:

- Auxiliary Output 1
- Auxiliary Output 2
- SMS Module

These signals are only generated when the “Arm / Disarm” menu option is set to “On”, the Auxiliary Outputs are set to “active” (if used) and or the SMS/MMS menu option is set to “On” (if used). **Reference Sections 7.05 (Arm / Disarm Alarms), 5.10 (Auxiliary Outputs) and 7.06 (SMS Module).**



Fig 7.07-2

- As an enrolled S-Admin, access the Advanced Settings menu by touching **MENU** on the keypad and verifying with the device.
- From the Advanced Settings menu, use the **▲** or **▼** keys to highlight the System Settings menu option. Touch **OK** to enter the System Settings menu.

- From the System Settings menu, use the **▲** or **▼** keys to highlight the Alarm Settings menu option. Touch **OK** to access the Alarm Settings menu.
- From the “Alarm Settings” menu, use the **▲** or **▼** keys to highlight the Event Linkage menu option. Touch **OK** to access the Event Linkage menu.
- From the Event Linkage menu, use the **▲** or **▼** keys to highlight the desired event and touch **OK** to access the sub menu for that event. **Reference Fig 7.07-1 as an example.**
- From the event sub menu, use the **▲** or **▼** keys to highlight the desired menu option and touch **MENU** to activate the desired option. One or all of the menu options can be activated. A green diamond will appear next to each option that has been activated. Touch **OK** to accept the changes. The “Setting Successful” screen will momentarily appear. **Reference Fig 7.07-2 as an example.**
- Touch **ESC** as necessary to exit all the menus.

7.08 AUX IN LINKAGE

In this menu option, each of the four Auxiliary Inputs can be set to generate an output signal at one or all of the following:

- Auxiliary Output 1
- Auxiliary Output 2
- SMS Module

These signals are only generated when the “Arm / Disarm” menu option is set to “On”, the Auxiliary Inputs are configured to detect the proper “high to low” or “low to high” transition, the Auxiliary Outputs are set to “active” (if used) and or the SMS/MMS menu option is set to “On” (if used).

Reference Sections 7.05 (Arm / Disarm Alarms), 5.11 (Auxiliary Inputs), 5.10 (Auxiliary Outputs) and 7.06 (SMS Module).

- As an enrolled S-Admin, access the Advanced Settings menu by touching **MENU** on the keypad and verifying with the device.
- From the Advanced Settings menu, use the **▲** or **▼** keys to highlight the System Settings menu option. Touch **OK** to enter the System Settings menu.

- From the System Settings menu, use the **▲** or **▼** keys to highlight the Alarm Settings menu option. Touch **OK** to access the Alarm Settings menu.
- From the Alarm Settings menu, use the **▲** or **▼** keys to highlight the Aux In Linkage menu option. Touch **OK** to access the Aux In Linkage menu. **(Fig 7.08-1)**
- From the Aux In Linkage menu, use the **▲** or **▼** keys to highlight the desired aux in linkage and touch **OK** to access the sub menu to set the input linkage.
- From the input linkage pop up menu, use the **▲** or **▼** keys to highlight the desired menu option and touch **MENU** to activate the desired option. One or all of the menu options can be activated. A green diamond will appear next to each option that has been activated. Touch **OK** to accept the changes. The “Setting Successful” screen will momentarily appear.
- Touch **ESC** as necessary to exit all the menus.



Fig 7.08-1

7.09 WIRELESS LINKAGE

In this menu option, the following sensor alarms (Perimeter, Smoke and Gas) can be set to generate an output signal at one or all of the following:

Auxiliary Output 1, Auxiliary Output 2 and the SMS Module. These signals are only generated when the “Arm / Disarm” menu option is set to “On”, the Auxiliary Outputs are set to “active” (if used) and or the SMS/MMS menu option is set to “On” (if used). **Reference Sections 7.05 (Arm / Disarm Alarms), 5.10 (Auxiliary Outputs) and 7.06 (SMS Module).**

- a) As an enrolled S-Admin, access the Advanced Settings menu by touching **MENU** on the keypad and verifying with the device.
- b) From the Advanced Settings menu, use the **▲** or **▼** keys to highlight the System Settings menu option. Touch **OK** to enter the System Settings menu.



Fig 7.09-1



Fig 7.09- 2

- c) From the System Settings menu, use the **▲** or **▼** keys to highlight the Alarm Settings menu option. Touch **OK** to access the Alarm Settings menu.
- d) From the “Alarm Settings” menu, use the **▲** or **▼** keys to highlight the Wireless Linkage menu option. Touch **OK** to access the Wireless Linkage menu. (**Fig 7.09-1**)
- e) From the Wireless Linkage menu, use the **▲** or **▼** keys to highlight the desired wireless sensor and touch **OK** to access the sub menu for that sensor. **Reference Fig 7.09-2 as an example.**
- f) From the wireless sensor sub menu, use the **▲** or **▼** keys to highlight the desired menu option and touch **MENU** to activate the desired option. One or all of the menu options can be activated. A green diamond will appear next to each option that has been activated. Touch **OK** to accept the changes. The “Setting Successful” screen will momentarily appear.
- g) Touch **ESC** as necessary to exit all the menus.

7.10 IMPACT SENSITIVITY

In this menu option, the Impact Sensitivity level can be changed from “Low” (where an alarm is triggered by a 300Hz vibration), to “Medium” (where an alarm is triggered by a 100Hz vibration) to “High” (where an alarm is triggered by a 40Hz vibration).

- a) As an enrolled S-Admin, access the Advanced Settings menu by touching **MENU** on the keypad and verifying with the device.
- b) From the Advanced Settings menu, use the **▲** or **▼** keys to highlight the System Settings menu option. Touch **OK** to enter the System Settings menu
- c) From the System Settings menu, use the **▲** or **▼** keys to highlight the Alarm Settings menu option. Touch **OK** to access the Alarm Settings menu.
- d) From the Alarm Settings menu, use the **▲** or **▼** keys to highlight the Impact Sensitivity menu option. Touch **OK** to access the Impact Sensitivity menu.
- e) Use the **▲** or **▼** keys to highlight the desired impact sensitivity level, “Low” “Medium” or “High”.
- f) Touch **OK** to accept the selected sensitivity level or touch **ESC** to discontinue the process and return to the Alarm Settings menu.

- g) When the impact sensitivity level has been changed, the “Setting Successful” screen will momentarily appear.
- h) Touch **ESC** as necessary to exit all the menus.

7.11 SETTING VERIFICATION MODES

Stone Lock® Pro allows you to configure four different verification modes

- 1:N Biometric Facial Recognition only
- 1:1 Biometric Facial Recognition with a card as a secondary verification method
- 1:1 Biometric Facial Recognition with a ID # number as a secondary verification method
- Card reader only

Stone Lock® Pro comes standard with HID iClass SE Card Reader hardware, allowing integration compatibility with a wide range of existing installations.

If a Stone Lock® Pro device is used as a stand-alone, and a card needs to be added or changed to an existing user record, the user profile must be selected, the card must be presented to the reader and the user must re-enroll.

If a Stone Lock® device is used with a fully integrated access control system or Stone Lock® Network (SLN) software, then cards can be added to profiles and uploaded.

This feature provides the capability to set the mode used for verification of a user in the Stone Lock® Pro device. The device can be set to “1:N” Biometric Facial Recognition only, “1:1” Biometric Facial Recognition with a secondary verification method (a card or a ID #), Mixed Mode where some users are allowed to authenticate with biometric only while other users are required to present a secondary form of verification (a card or an ID #), and “Card Only” which is card verification only.

- As an enrolled S-Admin, access the Advanced Settings menu by touching **MENU** on the keypad and verifying with the device.
- From the Advanced Settings menu, use the **▲** or **▼** keys to highlight the System Settings menu option. Touch **OK** to enter the System Settings menu.
- From the System Settings menu, use the **▲** or **▼** keys to highlight the Verification Mode menu option. Touch **OK** to access the Verification Mode menu. (**Fig 7.11-1**)
- Touch **ESC** as necessary to exit all the menus.

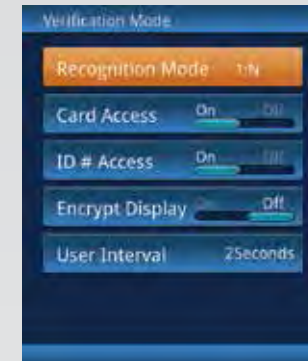


Fig 7.11-1

7.12 SETTING BIOMETRIC FACIAL RECOGNITION ONLY (1:N)



Fig 7.12-1



Fig 7.12-2

In the “1:N” mode, only biometric Facial Recognition can be used to gain access. When a face is detected, the system “wakes up” from the animation cycle to the Verifying screen. Using the same (non-expressive) face that was used during enrollment, the user should keep their face centered in the green frame of the verification screen. **(Fig 7.12-1)**

If the verification is successful, the device will momentarily display the “Successful” message screen.

After 2 seconds, if the device cannot verify the user, “Adjust to Enrolled Expression” will appear on the screen. After an additional 2 seconds, if the device still cannot authenticate the user “Denied” will appear on the screen and the device will file a verification failure record under “Denied Recs”. The device will continue to try to verify that person as long as he/she is present, repeating this cycle of messages over and over. **(See 4.02 Verification Failures)**

When a face is no longer detected, the device returns to the Animation Cycles.

Note: 1:N mode is the default mode for Stone Lock® Pro as shipped from the factory.

- As an enrolled S-Admin, access the Advanced Settings menu by touching **MENU** on the keypad and verifying with the device.
- From the Advanced Settings menu, use the **▲** or **▼** keys to highlight the System Settings menu option. Touch **OK** to enter the System Settings menu.
- From the System Settings menu, use the **▲** or **▼** keys to highlight the Verification Mode menu option. Touch **OK** to access the Verification Mode menu.
- From the Verification Mode menu, use the **▲** or **▼** keys to highlight the Recognition Mode menu option. Touch **OK** to enter the Modes menu.
- Use the **▲** or **▼** keys to highlight the “1:N” menu option. **(Fig 7.12-2)**
- Touch **OK** to accept the recognition mode or touch **ESC** to discontinue the process and return to the Verification Mode menu. The “Loading Biometric Profiles” screen will momentarily appear.
- When the recognition mode has been changed, the “Setting Successful” screen will momentarily appear.
- Touch **ESC** as necessary to exit all the menus.

7.13 SETTING BIOMETRIC FACIAL RECOGNITION WITH A SECONDARY VERIFICATION (1:1)

In the “1:1” mode, biometric facial recognition with a secondary verification method (either ID # or card) is required to be used to gain access. In this mode, the user enters an ID # or presents a valid card over the card symbol on the faceplate. If successful, an “Accepted” banner appears and the verifying screen is initiated comparing the user, 1:1, with the record registered to the ID # or card. If the person standing in front of the device matches the record referenced by the ID # or card, the verification is “Successful”.

When the Verification Mode is set to “1:1” with the “ID # Access” or “Card Access” menu option set to “On” in the “Verification Mode” menu, the system automatically switches from the Animation Cycle to the “Verifying” interface when one of the following occurs:

- a card is presented over the card symbol on the faceplate
- a face is detected
- any numeric key or **OK** is touched

A user must first enter their ID # or present their card prior to presenting their face for verification.

The device prompts the user to enter the ID # or present the card if the verifying screen has been activated. If the ID # or the presented card is associated with an existing user profile, the device will display the “Accepted” banner. If the ID # or

the presented card is NOT associated with an existing user profile, the device will display the “No User Information” banner.

Once the ID # or the card is confirmed, verification begins. Using the same (non-expressive) face that was used during enrollment, the user should keep their face centered in the green frame of the verification screen. If the verification is successful, the device will momentarily display the “Successful” message screen.

- a) As an enrolled S-Admin, access the Advanced Settings menu by touching **MENU** on the keypad and verifying with the device.
- b) From the Advanced Settings menu, use the **▲** or **▼** keys to highlight the System Settings menu option. Touch **OK** to enter the System Settings menu.
- c) From the System Settings menu, use the **▲** or **▼** keys to highlight the Verification Mode menu option. Touch **OK** to access the Verification Mode menu.
- d) From the Verification Mode menu, use the **▲** or **▼** keys to highlight either the “Card Access” or ID # Access menu option. Touch **OK** to toggle the graphical switch from “Off” to “On” or from “On” to “Off”. The “On” setting in either menu option allows that type of credential to be used as a secondary verification method to gain

access. The “Off” setting in either menu option does not allow that type of verification to be used as a secondary verification method.

Note: Either the “Card Access” or “ID # Access” menu option must be turned on prior to setting the “Recognition Mode” menu option to “1:1”. If both the “Card Access” and “ID # Access” menu options are set to “Off”, trying to set the “Recognition Mode” menu option to anything other than “1:N” will result in a “Settings Failed” message.

Note: If only one of the secondary verification methods (“Card Access” or “ID # Access”) is set to “On”, then that method is the required secondary verification method. If both secondary verification methods are set to “On”, then either method can be used as the secondary verification method. If the only secondary verification method is “Card Access”, the S-Admin SHOULD have a card tied to their profile prior to changing this setting in the event that the S-Admin forgets his/her ID#

- e) From the Verification Mode menu, use the **▲** or **▼** keys to highlight the Recognition Mode menu option. Touch **OK** to enter the “Modes” menu.
- f) Use the **▲** or **▼** keys to highlight the “1:1” menu option.
- g) Touch **OK** to accept the recognition mode or touch **ESC** to discontinue the process and return to the Verification Mode menu.
- h) When the recognition mode has been changed, the “Setting Successful” screen will momentarily appear.
- i) Touch **ESC** as necessary to exit all the menus.

7.14 SETTING MIXED MODE (1:N & 1:1)

Note: This mode should only be used when the device is connected to a fully integrated access control system or to the Stone Lock® Network (SLN) software application. Reference sections 2.3.1 Device Management and 2.4.4 User Management of the Stone Lock® Network User Guide

In the “Mixed” mode”, some users are allowed to authenticate with 1:N mode while remaining users are required to use it in 1:1.

- a) As an enrolled S-Admin, access the Advanced Settings menu by touching **MENU** on the keypad and verifying with the device.
- b) From the Advanced Settings menu, use the **▲** or **▼** keys to highlight the System Settings menu option. Touch **OK** to enter the System Settings menu.
- c) From the System Settings menu, use the **▲** or **▼** keys to highlight the Verification Mode menu option. Touch **OK** to access the Verification Mode menu.

- d) From the Verification Mode menu, use the **▲** or **▼** keys to highlight either the “Card Access” or “ID # Access” menu option. Touch **OK** to toggle the graphical switch from “Off” to “On” or from “On” to “Off”. The “On” setting in either menu option allows that type of credential to be used as a secondary verification method to gain access. The “Off” setting in either menu option does not allow that type of verification to be used as a secondary verification method.

Note: Either the “Card Access” or “ID # Access” menu option must be turned on prior to setting the “Recognition Mode” menu option to “Mixed”. If both the “Card Access” and “ID # Access” menu options are set to “Off”, trying to set the “Recognition Mode” menu option to anything other than “1:N” will result in a “Settings Failed” message.

Note: If only one of the secondary verification methods (“Card Access” or “ID # Access”) is set to “On”, then that method is the required secondary verification method. If both secondary verification methods are set to “On”, then either method can be used as the secondary verification method.

Note: If “ID # Access” is the only secondary verification method set to “On”, then all users that were enrolled by the device will be required to input their “ID#” prior to biometric facial recognition.

If the device is connected to a fully integrated access control system or to the Stone Lock® Network software application, then a mixed mode setting can be applied to specific users allowing them to verify by presenting face only, while other users who have not been set to mixed mode by the SLN will be required to input their “ID #” prior to biometric facial recognition.

Reference “Mixed Mode” in Section 2.4.4 User Management of the Stone Lock® Network User Guide.

- e) From the Verification Mode menu, use the **▲** or **▼** keys to highlight the Recognition Mode menu option. Touch **OK** to enter the Modes menu.
- f) Use the **▲** or **▼** keys to highlight the “Mixed” menu option.
- g) Touch OK to accept the recognition mode or touch **ESC** to discontinue the process and return to the Verification Mode menu.
- h) When the recognition mode has been changed, the “Setting Successful” screen will momentarily appear.
- i) Touch **ESC** as necessary to exit all the menus.

7.15 SETTING CARD ONLY

In the “Card Only” mode, the Stone Lock® Pro device operates as a fully functional card reader. The user presents a valid card over the card symbol on the faceplate, and if it is a card properly registered to the system, the verification is successful.

- a) As an enrolled S-Admin, access the Advanced Settings menu by touching **MENU** on the keypad and verifying with the device.
- b) From the Advanced Settings menu, use the ▲ or ▼ keys to highlight the System Settings menu option. Touch **OK** to enter the System Settings menu.
- c) From the System Settings menu, use the ▲ or ▼ keys to highlight the Verification Mode menu option. Touch **OK** to access the Verification Mode menu.

Note: The “Card Access” menu option must be in the “On” position and the “ID # Access” menu option must be in the “Off” position prior to setting the “Recognition Mode” menu option to “Card Only”. If the “Card Access” and “ID # Access” menu options are set in any other position, trying to set the “Recognition Mode” menu option to anything other than “1:N” will result in a “Settings Failed” message.

- d) From the Verification Mode menu, use the ▲ or ▼ keys to highlight the Card Access menu option. Touch **OK** to toggle the graphical switch from “Off” to “On” or from “On” to “Off”. Ensure that the switch is in the “On” position.
- e) From the Verification Mode menu, use the ▲ or ▼ keys to highlight the ID # Access menu option. Touch **OK** to toggle the graphical switch from “Off” to “On” or from “On” to “Off”. Ensure that the switch is in the “Off” position.
- f) From the Verification Mode menu, use the ▲ or ▼ keys to highlight the Recognition Mode menu option. Touch **OK** to enter the Modes menu.
- g) Use the ▲ or ▼ keys to highlight the “Card Only” menu option.
- h) Touch **OK** to accept the recognition mode or touch **ESC** to discontinue the process and return to the Verification Mode menu.
- i) When the recognition mode has been changed, the “Setting Successful” screen will momentarily appear.
- j) Touch **ESC** as necessary to exit all the menus.

7.16 ENCRYPTING THE USER INFORMATION UPON VERIFICATION

When the Encrypt Display menu option is set to “On”, the user information that is normally displayed on the LCD screen after a successful verification is replaced by “*”s to prevent other individuals who may be in the vicinity from seeing the user’s information.

- a) As an enrolled S-Admin, access the Advanced Settings menu by touching **MENU** on the keypad and verifying with the device.
- b) From the Advanced Settings menu, use the ▲ or ▼ keys to highlight the System Settings menu option. Touch **OK** to enter the System Settings menu.
- c) From the System Settings menu, use the ▲ or ▼ keys to highlight the Verification Mode menu option. Touch **OK** to access the Verification Mode menu.
- d) From the Verification Mode menu, use the ▲ or ▼ keys to highlight the Encrypt Display menu option. Touch **OK** to toggle the graphical switch from “Off to “On” or from “On” to “Off”.
- e) Touch **ESC** as necessary to exit all the menus.

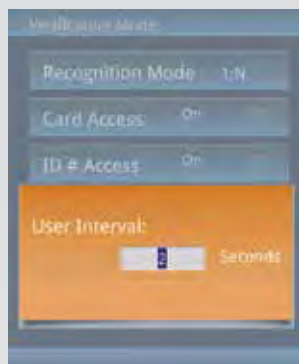


Fig 7.17-1

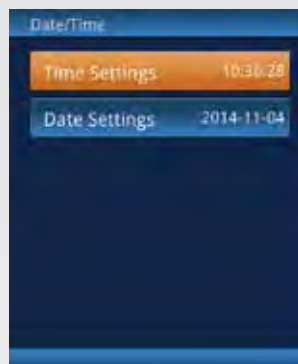


Fig 7.18-1

7.17 SETTING USER INTERVAL

The user interval is the amount of time between when a user has been verified and when that same individual is allowed to verify again.

- As an enrolled S-Admin, access the Advanced Settings menu by touching **MENU** on the keypad and verifying with the device.
- From the Advanced Settings menu, use the **▲** or **▼** keys to highlight the System Settings menu option. Touch **OK** to enter the System Settings menu.
- From the System Settings menu, use the **▲** or **▼** keys to highlight the Verification Mode menu option. Touch **OK** to access the Verification Mode menu.
- From the Verification Mode menu, use the **▲** or **▼** keys to highlight the User Interval menu option. Touch **OK** to access the User Interval menu.
- In the User Interval menu, enter the number of seconds for the interval up to 999999 seconds. Use the **◀** key to backspace if necessary. (**Fig 7.17-1**)
- Touch **OK** to accept the number or touch **ESC** to discontinue the process and return to the Verification Mode menu.

- When the User Interval has been accepted, the "Setting Successful" screen will momentarily appear.

- Touch **ESC** as necessary to exit all the menus.

7.18 DATE/TIME

This menu provides the capability to manually set the Date and Time of the Stone Lock® Pro device. If the device is connected to a fully integrated access control system or to the Stone Lock® Network (SLN) software application, its date and time can be synchronized with the server time.

- As an enrolled S-Admin, access the Advanced Settings menu by touching **MENU** on the keypad and verifying with the device.
- From the Advanced Settings menu, use the **▲** or **▼** keys to highlight the System Settings menu option. Touch **OK** to enter the System Settings menu.
- From the System Settings menu, use the **▲** or **▼** keys to highlight the Date/Time menu option. Touch **OK** to access the Date/Time menu. (**Fig 7.18-1**)
- Touch **ESC** as necessary to exit all the menus.

7.19 TIME SETTINGS

This menu provides the capability to manually set the Time of the Stone Lock® Pro device. If the device is connected to a fully integrated access control system or to the Stone Lock® Network (SLN) software application, its date and time can be synchronized with the server time.

- a) As an enrolled S-Admin, access the Advanced Settings menu by touching **MENU** on the keypad and verifying with the device.
- b) From the Advanced Settings menu, use the ▲ or ▼ keys to highlight the System Settings menu option. Touch **OK** to enter the System Settings menu.
- c) From the System Settings menu, use the ▲ or ▼ keys to highlight the Date/Time menu option. Touch **OK** to access the Date/Time menu.
- d) From the Date/Time menu, use the ▲ or ▼ keys to highlight the Time Settings menu option. Touch **OK** to access the Set Time menu. (*Fig 7.19-1*)
- e) Use the ▲ key to scroll from right to left and the ▼ key to scroll from left to right through the fields in the “Set Time” screen. From left to right, set the hour (in military time), the minute, and the second then touch **OK**.

The “Setting Successful” screen will momentarily appear.

- f) Touch **ESC** as necessary to exit all the menus.

7.20 DATE SETTINGS

This menu provides the capability to manually set the Date of the Stone Lock® Pro device. If the device is connected to a fully integrated access control system or to the Stone Lock® Network (SLN) software application, its date and time can be synchronized with the server time.

- a) As an enrolled S-Admin, access the Advanced Settings menu by touching **MENU** on the keypad and verifying with the device.
- b) From the Advanced Settings menu, use the ▲ or ▼ keys to highlight the System Settings menu option. Touch **OK** to enter the System Settings menu.
- c) From the System Settings menu, use the ▲ or ▼ keys to highlight the Date/Time menu option. Touch **OK** to access the Date/Time menu.
- d) From the Date/Time menu, use the ▲ or ▼ keys to highlight the Date Settings menu option. Touch **OK** to access the “Set Date” screen. (*Fig 7.20-1*)

- e) Use the ▲ key to scroll from right to left and the ▼ key to scroll from left to right through the fields in the “Set Date” screen. From left to right, set the year, the month and the day and then touch **OK**. The “Setting Successful” screen will momentarily appear.

- f) Touch **ESC** as necessary to exit all the menus.

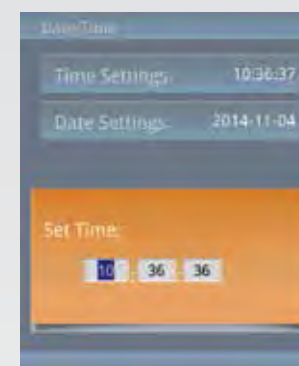


Fig 7.19-1

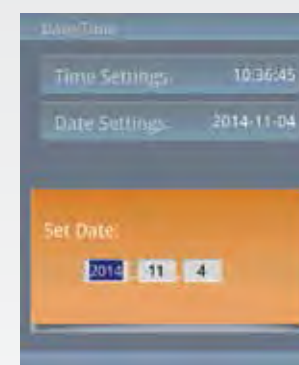


Fig 7.20-1

7.21 USB OPERATIONS

This feature provides the capability to upload software, download verification records, download user profiles and upload user profiles from a USB memory device.

- a) As an enrolled S-Admin, access the Advanced Settings menu by touching **MENU** on the keypad and verifying with the device.
- b) From the Advanced Settings menu, use the **▲** or **▼** keys to highlight the System Settings menu option. Touch **OK** to enter the System Settings menu.

Note: Prior to inserting a USB memory device, the USB Operations menu option is greyed out and is not accessible. The USB memory device must be no larger than 2GB and formatted to FAT32.



Fig 7.21-1

- c) Insert the USB memory device into the port located on the control device. At the bottom of the screen, the following 3 messages will be displayed, "USB Drive Has Been Detected...", "USB Drive Is Being Connected...", "USB Drive Is Connected...", followed by the USB Operations menu option becoming available.
- d) From the System Settings menu, use the **▲** or **▼** keys to highlight the USB Operations menu option. Touch **OK** to access the USB Operations menu shown in Fig 7.21-1.
- e) Touch **ESC** as necessary to exit all the menus.

7.22 PROGRAM UPDATE

This feature provides the capability to upload a different version of software to the Stone Lock® Pro device from a USB memory device. Program updates can also be performed via the network by using a fully integrated access control system or the Stone Lock® Network Software (SLN).

- a) As an enrolled S-Admin, access the Advanced Settings menu by touching **MENU** on the keypad and verifying with the device.
- b) From the Advanced Settings menu, use the **▲** or **▼** keys to highlight the System Settings menu option. Touch **OK** to enter the System Settings menu.

Note: Prior to inserting a USB memory device, the USB Operations menu option is greyed out and is not accessible. The USB memory device must be no larger than 2GB and formatted to FAT32.

- c) Insert the USB memory device into the port located on the control device. At the bottom of the screen, the following 3 messages will be displayed, "USB Drive Has Been Detected...", "USB Drive Is Being Connected...", "USB Drive Is Connected...", followed by the USB Operations menu option becoming available.
- d) From the System Settings menu, use the **▲** or **▼** keys to highlight the USB Operations menu option. Touch **OK** to access the USB Operations menu.
- e) From the USB Operations menu, use the **▲** or **▼** keys to highlight the Program Update menu option. Touch **OK** to upload the software.
- f) Once the upload is completed, the device should restart automatically. After 60 seconds if the device has not restarted, restart the device manually.
- g) Touch **ESC** as necessary to exit all the menus.

WARNING
Do not remove the USB memory device during the download process.

7.23 RECORDS DOWNLOAD

This feature provides the capability to download the verification records stored on the Stone Lock® Pro device to a USB memory device.

- a) As an enrolled S-Admin, access the Advanced Settings menu by touching **MENU** on the keypad and verifying with the device.
- b) From the Advanced Settings menu, use the ▲ or ▼ keys to highlight the System Settings menu option. Touch **OK** to enter the System Settings menu.

Note: Prior to inserting a USB memory device, the USB Operations menu option is greyed out and is not accessible. The USB memory device must be no larger than 2GB and formatted to FAT32.

- c) Insert the USB memory device into the port located on the control device. At the bottom of the screen, the following 3 messages will be displayed, “USB Drive Has Been Detected...”, “USB Drive Is Being Connected...”, “USB Drive Is Connected...”, followed by the USB Operations menu option becoming available.
- d) From the System Settings menu, use the ▲ or ▼ keys to highlight the USB Operations menu option. Touch **OK** to access the USB Operations menu.

- e) From the USB Operations menu, use the ▲ or ▼ keys to highlight the Records Download menu option.

- f) Touch **OK** to download the verification records. A progress bar showing the percent of completion will be displayed at the bottom of the screen. When the bar is gone, the download is complete.

WARNING
Do not remove the USB memory device during the download process.

- g) Touch **ESC** as necessary to exit all the menus.

7.24 USER DOWNLOAD

This feature provides the capability to download the user profiles stored on the Stone Lock® Pro device to a USB memory device.

- a) As an enrolled S-Admin, access the Advanced Settings menu by touching **MENU** on the keypad and verifying with the device.
- b) From the Advanced Settings menu, use the ▲ or ▼ keys to highlight the System Settings menu option. Touch **OK** to enter the System Settings menu.

Note: Prior to inserting a USB memory device, the USB Operations menu option is greyed out and is not accessible. The USB memory device must be no larger than 2GB and formatted to FAT32.

- c) Insert the USB memory device into the port located on the control device. At the bottom of the screen, the following 3 messages will be displayed, “USB Drive Has Been Detected...”, “USB Drive Is Being Connected...”, “USB Drive Is Connected...”, followed by the USB Operations menu option becoming available.
- d) From the System Settings menu, use the ▲ or ▼ keys to highlight the USB Operations menu option. Touch **OK** to access the USB Operations menu.
- e) From the USB Operations menu, use the ▲ or ▼ keys to highlight the User Download menu option.
- f) Touch **OK** to download the user profiles. A progress bar showing the percent of completion will be displayed at the bottom of the screen. When the bar is gone, the download is complete.

WARNING
Do not remove the USB memory device during the download process.

- g) Touch **ESC** as necessary to exit all the menus.

Notes:

7.25 USER UPLOAD

This feature provides the capability to upload the user profiles stored on a USB memory device to the Stone Lock® Pro device.

Note: Prior to inserting a USB memory device, the USB Operations menu option is greyed out and is not accessible. The USB memory device must be no larger than 2GB and formatted to FAT32.

- a) As an enrolled S-Admin, access the Advanced Settings menu by touching **MENU** on the keypad and verifying with the device.
- b) From the Advanced Settings menu, use the **▲** or **▼** keys to highlight the System Settings menu option. Touch **OK** to enter the System Settings menu. (*See Note at left.*)
- c) Insert the USB memory device into the port located on the control device. At the bottom of the screen, the following 3 messages will be displayed, "USB Drive Has Been Detected...", "USB Drive Is Being Connected...", "USB Drive Is Connected...", followed by the USB Operations menu option becoming available.

- d) From the System Settings menu, use the **▲** or **▼** keys to highlight the USB Operations menu option. Touch **OK** to access the USB Operations menu.
 - e) From the USB Operations menu, use the **▲** or **▼** keys to highlight the User Upload menu option.
 - f) Touch **OK** to upload the user profiles. A progress bar showing the percent of completion will be displayed at the bottom of the screen. When the bar is gone, the upload is complete.
- WARNING**
Do not remove the USB memory device during the download process.
- Note:** User profiles on the USB memory device which have different ID#s than those which already reside on the device will be added to the profiles on the device. Any user profile on the USB memory device which has the same ID# as one which already resides on the device will overwrite the profile on the device.
- g) Touch **ESC** as necessary to exit all the menus.

Section 8: System Info



8.01 System Info

Section 8: System Info



Fig 8.01-1



Fig 8.01-2

8.01 System Info

The System Info menu provides the user with the ability to change the language used for the menus as well as provide information about the Device S/N, the software version installed on the device, the amount of disk space used verses the amount available, the number of 1:N users enrolled verses the maximum number of 1:N users allowed and the total number of users enrolled verses the maximum number of 1:1 users allowed.

- As an enrolled S-Admin, access the Advanced Settings menu by touching **MENU** on the keypad and verifying with the device.
- From the Advanced Settings menu, use the **▲** or **▼** keys to highlight the System Info menu option. Touch **OK** to enter the System Info menu shown in **Fig 8.01-1**.
- From the System Info menu, Touch **OK** to access the Languages: menu. (**Fig 8.01-2**)
- Use the **▲** or **▼** keys to highlight the desired language: “Simplified Chinese”, “English”, or “Traditional Chinese”.
- Touch **OK** to accept the selected language or touch **ESC** to discontinue the process and return to the System Info menu.
- When the language has been changed, the “Setting Successful” screen will momentarily appear.
- Touch **ESC** as necessary to exit all the menus.

Section 9: Appendices

9.01 Troubleshooting

9.02 Product Specifications

9.03 Dimension Drawings

9.04 Warranty

9.01 Troubleshooting

In the event this section does not help you correct a problem with your Stone Lock® Pro device, please contact your integrator or CoprometroUSA® at support@coprometrousa.com or (913) 998-6168.

Problem	Suggestion
Alarm Device Connected to Auxiliary Output 1 or 2 Doesn't Activate	1. Verify the desired Event Linkage, Aux In Linkage or Wireless Linkage in the Advanced Settings/System Settings/Alarm Settings/Event Linkage submenu has been set to "Output 1" or "Output 2". Reference Sections 7.04 and 7.09
	2. Verify the "Arm / Disarm" menu option in the Advanced Settings/System Settings/Alarm Settings sub menu is set to "ON". Reference Section 7.05
	3. Verify the wiring between the control device and the alarm device.
	4. Verify that the alarm device is functioning properly.
Device Periodically Restarts In Dual Faceplate Application	1. Verify that the RJ45 connector in Front 1 on the Control Device and on Faceplate 1 is fully seated and locked in place.
	2. Verify that the communication cable (Cat5/5e/6) between the Front 1 on the Control Device and on Faceplate 1 is good. Verify that the wires have been properly placed in the RJ45 connectors (in accordance with standard TIA/EIA 568b) are properly crimped in the RJ45 connectors and the continuity of each wire is good.
Device Fails To Switch from the Standby Screen To Recognition Interface	1. The user is not facing directly at the device
	2. Sunlight is shining directly into the device or over the shoulder of the user. Reference Section 1.08
	3. Verify that the "Silent Alarm" feature is "Off". Reference Section 5.13
Device Powers Up Temporarily	Verify that the voltage at the control device is not greater than 13.8 VDC.

Problem	Suggestion
Device Restarts, LCD Display Distorts or Turns Blue	If the device operates normally in the standby screen but during verification and/or the activation of subsequent functions (door lock actuation, use of auxiliary outputs etc.) the device restarts, or the Faceplate LCD display distorts or turns blue:
	1. Verify that the power supply voltage has been set properly to compensate for the cable distance between the power supply and the device. Reference Section 1.04 and 1.13 of this manual.
	2. Verify that the voltage at the connector on the control device stays within the specified limits before and during verification.
	3. Verify that the power supply is capable of supplying sufficient amperage for the application. Use the “Stone Lock® Pro Functions/Configuration” table to determine the maximum current draw by the device. Reference Section 1 of this manual for power supply specifications.
	4. Verify that the RJ45 connector on the Control Device and on the Faceplate is fully seated and locked in place.
	Use the “Stone Lock® Pro Functions/Configuration” table to determine the maximum current draw by the device. Reference Section 1.04 and 1.13 of this manual.
Device Switches to Recognition Interface but Verification Process Fails to Start	If the device recognizes that a face is present and the infrared LEDs turn on but it does not begin the verification process indicated with the green scanning bar:
	1. Verify that the user is facing directly at the device, centered in the screen and within the appropriate height and distance requirements (approximately 3 to 4 feet).
	2. Verify that the RJ45 connector on the Control Device and on the Faceplate is fully seated and locked in place.
	3. Verify that the communication cable (Cat5/5e/6) between the Control Device and the Faceplate is good. Verify that the wires have been properly placed in the RJ45 connectors (in accordance with standard TIA/EIA 568b) are properly crimped in the RJ45 connectors and the continuity of each wire is good.
	4. The communication handshake between the control device and the Faceplate has been disrupted. Power down the control device, wait for 5 seconds and restart the control device.
	5. If after restarting the device, the problem persists, the Faceplate may be malfunctioning. Contact support@coprometrousa.com.
Enrolled User Is Denied When Device Is Set To Mixed Verification Mode	Verify that the user has been set up for mixed verification mode using a fully integrated access control system or the Stone Lock® Network (SLN) Software. Reference Section 7.14 Setting Mixed Mode (1:N & 1:1).

9.01 Troubleshooting

Problem	Suggestion
Enrolled User is Denied When Device Is Set To 1:N Verification Mode	1. Verify that the user is using the same expression that they enrolled with.
	2. Extremely thick lenses, bifocals, trifocals, safety glasses, sun glasses or dark transitional glasses may cause problems.
	3. Something has changed about the user since the enrollment or since the last time the user verified at the unit (ex. Glasses, cosmetic surgery, trauma or other extreme changes).
	4. The original enrollment was not performed well. Reference “Preparation for User Enrollment” in Section 3.02, New User Enrollment before re-enrolling the user.
Facial Recognition Infrared LEDs Fail to Activate	If the facial recognition infrared LEDs fail to activate but the face detection infrared LEDs are still operational:
	1. Verify that the RJ45 connector on the Control Device and on the Faceplate is fully seated and locked in place.
	2. Verify that the communication cable (Cat5/5e/6) between the Control Device and the Faceplate is good. Verify that the wires have been properly placed in the RJ45 connectors (in accordance with standard TIA/EIA 568b) are properly crimped in the RJ45 connectors and the continuity of each wire is good.
	3. The communication handshake between the control device and the Faceplate may have been disrupted. Power down the control device, wait for 5 seconds and restart the control device.
	4. If 1 through 3 have been tried and the Faceplate presents the green scanning bar and tries to authenticate the user, the Faceplate address may be incorrectly set. Reference 1.11 Setting the Faceplate Address.
	5. If 1 through 4 have been tried, then the Faceplate or the control device may have been damaged. Contact support@coprometrousa.com.

Problem	Suggestion
Faceplate Alarm Sounds a Combination of Long and Short Beeps	Enter the menu system and set the Impact Sensitivity to “Low”. If the alarm continues to sound, the impact sensitivity sensor may be malfunctioning. Contact support@coprometrousa.com. Reference Section 7.10
Faceplate Alarm Sounds Quick Short Beeps	Verify that the anti-tamper alarm reflector has been installed and is in the proper position.
Keypad Slow or Stays Lit	Verify that the voltage measured at the Faceplate is steady between 7.5 VDC and 13.8 VDC before and during verification
Keypad Unresponsive	1. Verify that the RJ45 connector on the Control Device and on the Faceplate is fully seated and locked in place.
	2. Verify that the communication cable (Cat5/5e/6) between the Control Device and the Faceplate is good. Verify that the wires have been properly placed in the RJ45 connectors (in accordance with standard TIA/EIA 568b) are properly crimped in the RJ45 connectors and the continuity of each wire is good.
	3. The communication handshake between the control device and the Faceplate has been disrupted. Power down the control device, wait for 5 seconds and restart the control device.
	4 The keypad is malfunctioning. Contact support@coprometrousa.com.
LCD Display Intermittently Showing Green Adjustment Bar	Verify that the voltage measured at the Faceplate is steady between 7.5 VDC and 13.8 VDC before and during verification. The green adjustment bar is intermittently present on the Faceplate LCD display when the voltage at the Faceplate is low or is fluctuating and unstable. It is an indication that the Faceplate is attempting to adjust its color and contrast. If the voltage continues to fluctuate, the screen may adjust to black and white.

9.01 Troubleshooting

Problem	Suggestion
LCD Display Has a Blue Screen	1. Verify that the RJ45 connector on the Control Device and on the Faceplate is fully seated and locked in place.
	2. Verify that the communication cable (Cat5/5e/6) between the Control Device and the Faceplate is good. Verify that the wires have been properly placed in the RJ45 connectors (in accordance with standard TIA/EIA 568b) are properly crimped in the RJ45 connectors and the continuity of each wire is good.
	3. If the Faceplate is NOT powered by the control device but powered separately, then verify that the Control Device has not lost power.
	4. If items 1 through 3 have been verified and the voltage measured at the Faceplate is between 7.5 VDC and 13.8 VDC before and during verification, then the Faceplate or the control device may have been damaged. Contact support@coprometrousa.com.
LCD Display Not Lit	1. Verify that you have the appropriate voltage at the input of the Control Device. Reference Section 1.04 and 1.13 of this manual.
	2. Verify that the 2 pin connectors on the Control Device and on the Faceplate are properly seated.
	3. Verify that the wires at the 2 pin connectors on the Control Device and on the Faceplate are NOT loose or have been stripped back to far and are touching.
	4. Verify that the corresponding wire connected to the “Power Out” pin on the control device is connected to the “+12V” pin on the Faceplate and corresponding wire connected to the “GND” pin on the control device is connected to the “GND” pin on the Faceplate.
	5. If items 1 through 4 have been verified and the voltage measured at the Faceplate is between 7.5 VDC and 13.8 VDC before and during verification, then the Faceplate may have been damaged. Contact support@coprometrousa.com.
LCD Display Is Black and White	Verify that the voltage measured at the Faceplate is steady between 7.5 VDC and 13.8 VDC before and during verification. When the voltage at the Faceplate fluctuates for a period of time, the LCD display may adjust to black and white.

Problem	Suggestion
LCD Display Exhibits Sporadic Color Video	1. The faceplate is too far from the Control Device. <i>Reference Section Sections 1.07 and 1.08.</i>
LCD Display Prompts “No Color Video”	2. The Faceplate or the control device may have been damaged. Contact support@coprometrousa.com.
LCD Display Turns Dark, Exhibits Distortion, Exhibits Clear Ripples In Standby Interface	If the LCD Display:
	1. turns dark
	2. exhibits distortion or
	3. exhibits clear ripples when the device is in the standby interface, and the ripples become bigger when a card is read or a key is touched
	Verify that the voltage measured at the Faceplate is steady between 7.5 VDC and 13.8 VDC before and during verification.
Normal Color Video but Device Won’t Enroll or Verify Users	1. Verify that the RJ45 connector on the Control Device and on the Faceplate is fully seated and locked in place.
	2. Verify that the communication cable (Cat5/5e/6) between the Control Device and then Faceplate is good. Verify that the wires have been properly placed in the RJ45 connectors (in accordance with standard TIA/EIA 568b) are properly crimped in the RJ45 connectors and the continuity of each wire is good.
	3. The communication handshake between the control device and the Faceplate has been disrupted. Power down the control device, wait for 5 seconds and restart the control device.
	4. The IR Camera may be malfunctioning. Contact support@coprometrousa.com.

9.01 Troubleshooting

Problem	Suggestion
Lock Doesn't Unlock After Successful Verification	1. Verify that the Device Permission in the Access Control Menu has been set to Access. <i>Reference Section 5.02.</i>
	2. Verify that the Lock #1 and/or Lock #2 in the Door Settings menu is set to a. "Active" if powering a 12VDC Lock b. "Passive" if the lock is powered by a separate supply c. "Electric" if the lock is motor controlled. <i>Reference Sections 5.03 and 5.04.</i>
	3. Verify the continuity in the wiring from the device to the locks.
	4. Verify that the wires are properly seated in the screw connectors.
	5. Because the individual user permissions take precedence over the Device Permission, verify that the verification records for the user indicates "Access confirmed" and not just "Verification success". If the verification records show "successful verification", use a fully integrated access control system or the Stone Lock® Network (SLN) Software to set the users permission to open the lock.
Lock Works In Reverse	If the lock unlocks when the device powers up and then locks after a successful verification, verify that the wiring is correct to the Electronic Lock Outputs (example, the "Close1" pin is being used instead of the "Open1" pin).
SD Card Undetected or Invalid Serial Number	If the Faceplate LCD display prompts "SD Card Undetected" or "Invalid Serial Number", contact support@coprometrousa.com.

Problem	Suggestion
Mobile Device Doesn't Receive SMS Or MMS Messages <i>Note: Only Available in Select Markets</i>	Note: When the Event Linkages of Denied User:, Faceplate Removed, or Impact Alarms are set, triggering of these alarms will be sent via MMS. All other alarms are sent via SMS.
	- Verify the "SMS/MMS" menu option in the Advanced Settings/System Settings/Alarm Settings submenu is set to on. Reference Section 7.06. - Verify the Mobile ID#(s) have been correctly entered in the Advanced Settings/System Settings/Alarm Settings submenu. - Verify the desired Event Linkage, Aux In Linkage or Wireless Linkage in the Advanced Settings/System Settings/Alarm Settings/Event Linkage submenu has been set to "SMS". - Verify the "Arm / Disarm" menu option in the Advanced Settings/System Settings/Alarm Settings submenu is set to "ON". Reference Section 7.05. - Verify the SIM card is correctly seated in its slot. - Verify the cellular account is operational and the SMS and MMS functions are NOT blocked. If the account has expired, once the account has been reactivated restart the device. If MMS messages are being received from Denied User:, Faceplate Removed, or Impact Alarms but SMS messages are not being received, the GPRS for the account needs to be activated.
Problems with Facial Recognition Infrared LEDs in Dual Faceplate Applications	If the facial recognition infrared LEDs fail to activate for the Faceplate where verification is taking place but instead come on for the opposite Faceplate, the Faceplate that should have been connected to Front 1 has been connected to Front 2 and vice-versa Reference 1.11 Setting the Faceplate Address
	If the facial recognition infrared LEDs activate for both faceplates during verification at Faceplate 1, the address for Faceplate 2 may be incorrectly set to the same Front 1 address as Faceplate 1. Reference 1.11 Setting the Faceplate Address
	If the facial recognition infrared LEDs activate for both faceplates during verification at Faceplate 2, the address for Faceplate 1 may be incorrectly set to the same Front 2 address as Faceplate 2. Reference 1.11 Setting the Faceplate Address
	If Faceplate 2 facial recognition infrared LEDs activate when verifying at Faceplate 2 but Faceplate 1 facial recognition infrared LEDs DO NOT activate when verifying at Faceplate 1, the address for Faceplate 1 may be incorrectly set to a Front 2 address that is different than the address of Faceplate 2. Reference 1.11 Setting the Faceplate Address

9.02 Product Specifications

Capacity

Single Unit - 1,000 1:N profiles
- 10,000 1:1 profiles
- 300,000 Maximum stored verification records

Networked - 1:1 no limit*

**Requires LAN with server running Stone Lock® Network Software or an enterprise platform - visit www.stonelockpro.com for details*

Card Reader -

Supports MIFARE Classic®, MIFARE DESFire® 0.6, MIFARE DESFire® EV1, HID: iCLASS® Standard/SE/SR/Seos; PIV II, Secure Identity Object™ (SIO), 35 Bit Corporate 1000, 37 Bit and 37 Bit infinity Card Formats

Enrollment

Approximately 15 seconds / user

Measurements

2,165 Points

Speed

Measurement time < 10ms
Record match time < 0.002ms

False Acceptance Rate (FAR)

FAR: Better than 1 in a quarter million
1/250,000 (< 0.0004%) at highest sensitivity

Ambient Light Range

0-6000 Lx

Temperature

25°C - 55°C (-10°F - 130°F)

Moisture

20% RH - 95% RH

Connectivity

Wiegand, RS485, USB, Cat5/5e/6 Ethernet

(Wiegand may be set to Card #, User ID #, or Custom #)

2 Form C Contacts

Electrical Requirements

12.0 VDC $\pm$ 1.8 VDC, ($\pm$ 15%)
measured at the unit

2 Amps Min, some configurations
may draw up to 11 Amps

Refer to Stone Lock® Pro User
Guide for specifics

Impact Sensitivity Settings

Low – Alarm triggered by a 300Hz
vibration

Medium – Alarm triggered by a 100Hz
vibration

High – Alarm triggered by a 40Hz
vibration

LCD Screen

3.5" TFT Display

Body

Aluminum uni-body design

Electronic Locks 1 and 2

Active Mode - Approximately 12VDC output
(voltage equivalent to the
supply voltage minus 0.3
VDC), 2 Amps Maximum
Output

Passive Mode - Form C contacts, Maximum
24VDC at 10 Amps,
DOES NOT SUPPORT AC
SIGNALS.

Auxiliary Output 1 and 2

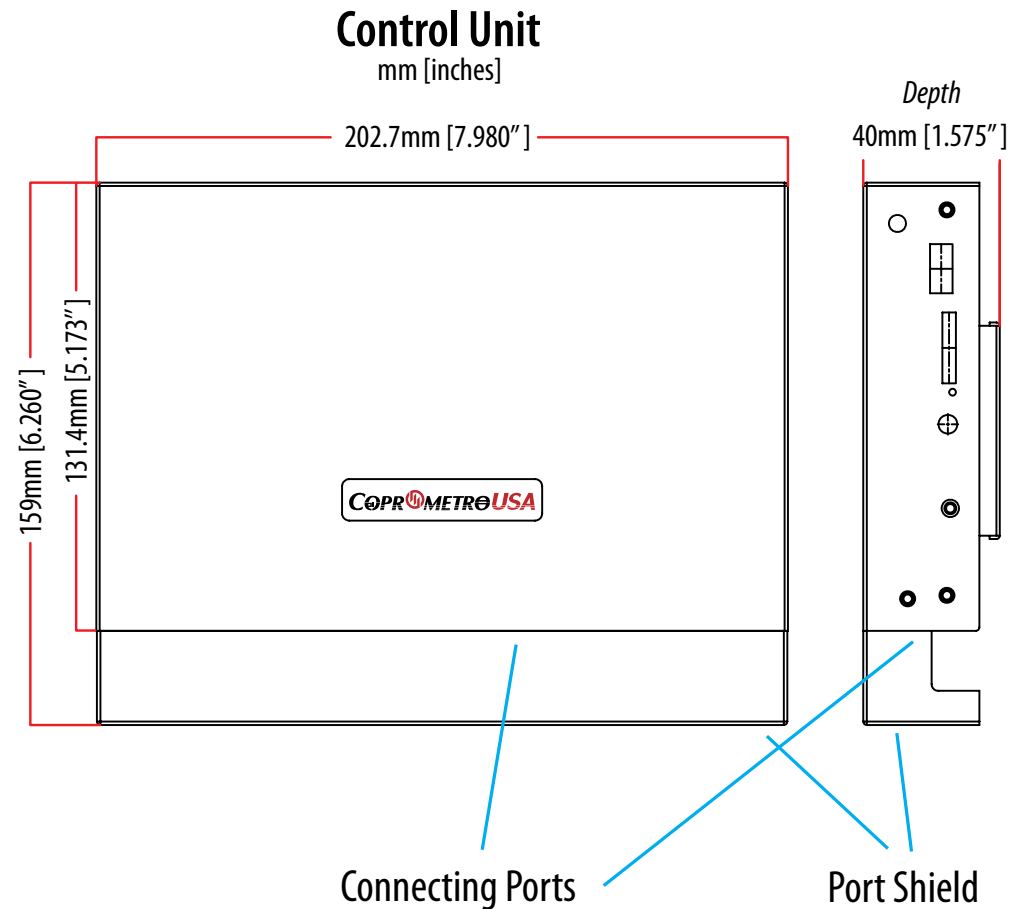
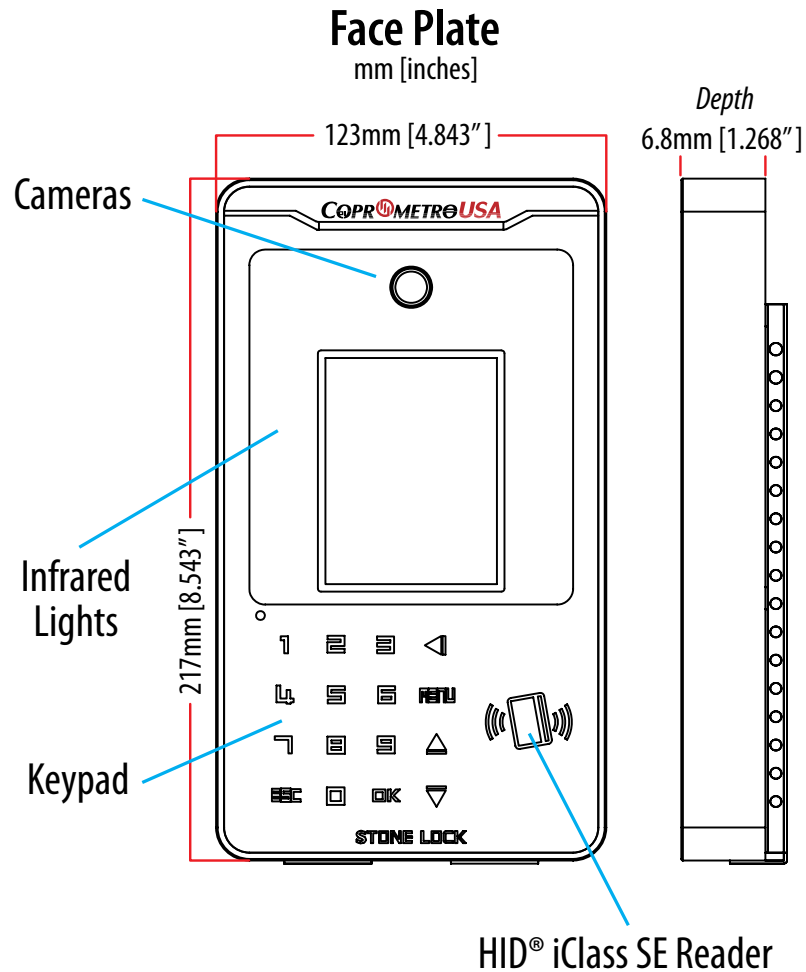
Active Mode - Approximately 12VDC output
(voltage equivalent to the
supply voltage minus 0.3
VDC), 2 Amps Maximum
Output

Passive Mode - Form C contacts, Maximum
24VDC at 10 Amps,
DOES NOT SUPPORT AC
SIGNALS.

Auxiliary Output Power (PIN 19)

Approximately 12VDC output (voltage
equivalent to the supply voltage), 1 Amp
Maximum Output.

9.03 Dimension Drawings



9.04 Warranty & Return Policy

2-YEAR LIMITED WARRANTY

- 1 CoprometroUSA® warrants to the original purchaser of Stone Lock® Pro (“product”) that the product will be free from defects in workmanship and materials under normal use for a period of two (2) years from the date that the product is shipped to the original purchaser.
- 2 During the warranty period, defective product will be replaced without charge at CoprometroUSA’s sole discretion. This limited warranty covers the replacement of the defective product only.
- 3 This limited warranty does not apply when the product is opened or repaired by someone not authorized by CoprometroUSA®.
- 4 This limited warranty does not cover repair or replacement of any product damaged by: misuse, moisture, liquids, proximity or exposure to heat and accident, abuse, non-compliance with the instructions supplied with the product, neglect or misapplication.
- 5 This limited warranty does not cover physical damage to the surface of the product.
- 6 This limited warranty does not cover any damage to the unit caused by the installation of unauthorized software.
- 7 This limited warranty does not cover the installation, removal or maintenance of the Hardware or any costs related herewith.
- 8 This limited warranty gives the original purchaser specific legal rights; original purchaser may also have other rights, which vary from state to state and jurisdiction to jurisdiction.

RETURN POLICY

In order to make a claim of a defective unit, you must:

- 9 Contact CoprometroUSA® (phone or email below) during the warranty period to explain the defect and to obtain an RMA number (Return Materials Authorization).
- 10 CoprometroUSA® will send a replacement unit within 1 business day of issuing an RMA.
- 11 User must return the questionable product within 5 business days of receipt of the replacement unit to avoid invoicing of the replacement.
- 12 Evaluation and disposition of the questionable unit will be reported within 30 days of receipt of unit.
- 13 User may be required to comply with other return procedures stipulated by CoprometroUSA®, if any.

COPROMETROUSA®

Coprometro, Inc.

1-913-998-6168 • support@coprometrousa.com



COPROMETROUSA®

Coprometro, Inc.

1-913-998-6168 • support@coprometrousa.com • www.stonelockpro.com

Rev 04.01.15